PRIRUČNIK

Internet of Things

RAZVOJ INTELIGENTNIH **IoT** APLIKACIJA

ALDI SKILL ACCELERATOR
AITI-IOT-001-180

PRIRUČNIK

Internet of Things

RAZVOJ INTELIGENTNIH IOT APLIKACIJA

Sadržaj

ALDI INICIJATIVA ZA INOVATIVNI TRENING
INTERNET OF THINGS (INTERNET STVARI)
Izgradnja inteligentnih IoT aplikacija
PRIRUČNIK ZA POLAZNIKE
Kurs AITI-IOT-001-180
PRVO IZDANJE
JUNI 2020
Udruženje za lokalne razvojne inicijative
(ALDI)
Panorama b.b.
Goražde
BH 73000
Bosna i Hercegovina
aldi@aldi.ba
www.aldi.ba

05

PREDGOVOR

INTERNET OF THINGS

Razvoj inteligentnih IoT aplikacija

06

PREGLED PROGRAMA

AITI-IOT-001-180

Razvoj inteligentnih IoT aplikacija

7

UVOD

TRANSFORMACIJA IOT

Kako iskoristiti puni potencijal IoT

13

PRVO POGLAVLJE

KOMUNIKACIJSKE VJEŠTINE

253

TREĆE POGLAVLJE

MENADŽMENT KOMUNIKACICJA

381

ČETVRTO POGLAVLJE

VJEŠTINE PREZENTIRANJA

ALDI

Skill Accelerator

Follow us at @UAITLab

Internet of Things

Razvoj inteligentnih IoT aplikacija

Internet of Things (Internet stvari) je jedna od tehnologija koja ubrzano evolvira posljednjih pet godina i koja je svrstana u ključne faktore razvoja inteligentnih proizvoda, kuća, preduzeća i gradova.

IoT je zajedno sa vještačkom inteligencijom i naprednom analitikom digitalna tehnologija koja transformiše načine na koji danas živimo i radimo.

Krajem 2019. godine Udruženje ALDI je provelo istraživanje među mladim visokoobrazovanim osobama kako bi saznalo koje od ove tri tehnologije smatraju da mogu imati najveću ulogu u budućem digitalnom dobu.

Odgovor je bio skoro jednoglasan: IoT.

To nije nimalo iznenađujuće. IoT ne samo da je sve popularnija tehnologija, već i sve pametnija. Integracija IoT u digitalni ekosistem omogućava ovoj tehnologiji da koristi prednosti koje donosi vještačka inteligencija i napradna analitika stvarajući IoT aplikacije koje imaju unaprijeđenu operativnu efikasnost i koje doprinose generisanju podataka na osnovu kojih kompanije mogu dobivati korisne uvide koji su ključni za donošenje poslovnih odluka.

Ove promjene dovele su do niza novih proizvoda i sve veću primjenu IoT u kompanijama. Zahvaljujući novim sposobnostima IoT, kompanije ubrzano izrađuju IoT strategije i prave procjene kako potencijalni inteligentni IoT sistemi mogu doprinijeti poboljšanju njihove konkurentske prednosti na tržištu.

Procjenjuje se da će do 2025. godine u funkciji biti preko 45 milijardi IoT uređaja koji će pokretati pametne gradove, pametne kuće, transformisati tradicionalne industrijske sektore, i donijeti brojne nove mogućnosti svim područjima života i rada.

Koliko će se iskoristiti mogućnosti koje donosi IoT značajno zavisti od kapaciteta pojedinaca i organizacija da iskoriste potencijale koje donosi ova tehnologija. Kako bi doprinijeli tim naporima, AITI je razvio specijaliziran program obrazovanja koji vam može pomoći da steknete neophodni set znanja i vještina ključnih za planiranje i razvoj inteligentnih IoT aplikacija, spremnih za primjenu u stvarnom životu.

Ovaj Priručnik je kreiran da bi vam olakšao vaše putovanje u svijet inteligentnih IoT aplikacija. On će vam pomoći da razumijete osnovne procese, alate i tehnike koje se koriste u razvoju IoT aplikacija, da razumijete mogućnosti IoT na osnovu kojih možete razviti poslovne ideje i razviti hardver koji će fizičke stvari konektovati na internet i koje će biti sastavni dio inteligentne IoT aplikacije.

Goražde, 30.06.2020. godine

Pregled programa

Internet of Things

Kurs: AITI-IOT-001.180
Naziv kursa: Internet of Things
Pregled: Broj časova po modulima

Oznaka modula	Naziv modula	Teorija	Vježbe	Lab	Ukupno
IOT-INTRO.	Uvod u IoT	3	0	3	6
IOT-NC2.	IoT hardver	6	8	0	14
KIP-NC3.	Komunikacijski proces	5	4	4	13
KIP-NC4.	Napredne prezentacijske vještine	9	10	15	34
	UKUPNO SATI	**23**	**25**	**19**	**67**

Već smo rekli da je Internet of Things skup različitih senzora, uređaja i drugih tehnologija međusobno povezani internetom koji pomažu ljudima u pružanju informacija i kontrole Sa pojavom jeftinih senzora i niske cijene povezivanja, IoT tehnologije postaju sve raširenije i pristupačnije za kompanije bilo velike ili male.

Ovo je samo jedan od razloga zbog kojih broj kompanija koje investiraju u IoT postaje sve veći, a na hiljade kompanija već stiću transformacijske koristi od ove tehnologije. Ali još uvijek daleko je veći broj onih kompanija koje se bore sa ključnim izazovima IoT, uključujući potrebu za višom fleksibilnošću, većom sigurnošću, boljem iskorištavanju IoT podataka i sposobnošću da se adresiraju nove korisničke potrebe.

Prilikom uvođenja IoT tehnologija mnogi brzo saznaju da jednostavno povezivanje „stvari“ na Internet nije dovoljno. Da bi IoT donio stvarnu transformaciijsku promjenu on mora osigurati da se podaci koje generišu „stvari“ mogu iskoristiti na način koji donosi nove poslovne koristi.

Bilo da je korist reduciranje poslovnih troškova ili poboljšanje korisničkog iskustva sa novom uslugom, sistem koji pokreće IoT da bi bio efikasan mora na inteligentan način iskoristiti podatke koje prikuplja. Zbog toga nije čudo što su kompanije preplavljene podacima koji dolaze od IoT uređaja i što sve veći broj rješenja uključuuje AI kako bi im pomogao u upravljanju uređajima, kao i u tome da steknu korisne uvide iz ogromne količine prikupljenih podataka.

Međutim, mnogo je teže upravljati i izvlačiti vrijedne informacije iz ovih sustava nego što bismo mogli očekivati. Na IoT postoji mnogo aspekata i komponenti kao što su povezanost, sigurnost, pohrana podataka, integracija sistema, hardver uređaja, razvoj aplikacija, pa čak i mreže i procesi koji se u ovom prostoru stalno mijenjaju. Drugi sloj komplikacija s IoT-om ima veze sa opsegom funkcionalnosti. Često je lako izgraditi senzore kojima se pristupa sa pametnog uređaja, ali stvoriti uređaje koji su pouzdani, daljinski upravljani i nadograđeni, sigurni i ekonomičniji je mnogo složenija stvar.

Kako napraviti inteligentni IoT

Sa sve raširenijom primjenom AI, logično je bilo da će ubrzo doći do integracije ove dvije tehnologije koje po mnogima imaju najveću snagu za transformaciju. Kombinacija AI i IoT nalazi svoju primjenu kako bi se osigurala veća vidljivost i kontrola nad širokim nizom uređaja i senzora povezanih s internetom. Na razvoju rješenja koja kombinuju IoT i AI, rade kompanije svih vrsta, od vodećih tehnoloških giganata kao što su Amazon, Google, Microsoft i IBM, do proizvođača uređaja, programera aplikacija, integratora sustava i

ostalih vertikalno fokusiranih partnera koji daju svoj doprinos u integraciji ove dvije tehnoologije kako bi IoT osigurato stransformativnun vrijednost za biznise.

Cilj ovih napora je fokusiran na stjecanje uvida i znanja iz podataka koji su stvoreni s IoT uređaja, pojednostavljujući pristup i izvještavanje tih podataka.

IoT transformira poslovne modele pomažući tvrtkama da prijeđu od naprosto izrade proizvoda i usluga do tvrtki koje svojim kupcima daju željene rezultate. Utječući na poslovne modele organizacija, kombinacija uređaja i senzora koji omogućuju IoT s strojnim učenjem stvara suradnički i međusobno povezan svijet koji se usklađuje oko rezultata i inovacija. Ta kombinacija IoT i AI mijenja mnoge industrije i odnose koje tvrtke imaju sa svojim kupcima. Poduzeća sada mogu putem IoT-a prikupljati i pretvarati podatke u korisne i vrijedne informacije.

Kako organizacija primjenjuje principe digitalne transformacije u svom poslovanju, kombinacija IoT-a i AI-a može stvoriti poremećaj unutar njegove industrije. Bez obzira koristi li organizacija IoT i AI kupce, implementira konverzacijske agente za kupce, prilagođava korisničko iskustvo, dobiva analitiku ili optimizira produktivnost uvidima i predviđanjima, korištenje IoT i AI stvara dinamiku u kojoj tvrtke mogu dobiti visoku kvalitetu uvid u svaki dio podataka, od onoga što kupci zapravo gledaju i dodiruje kako zaposlenici, dobavljači i partneri komuniciraju s različitim aspektima ekosustava. Umjesto da poslovne procese modeliraju u softveru na način koji približava stvarnom svijetu, IoT uređaji daju sIstemima stvarni interfejs u stvarnom svijetu.

Na svako mjesto gdje možete staviti senzor ili uređaj za mjerenje, interakciju ili analizu nečega, možete staviti IoT uređaj spojen na inteligentnu aplikaciju koja podržava AI kako biste dodali značajne količine vrijednosti u vidu korisnih uvida iz podataka koje IoT uređaji prikupljaju.

Ne brinite se ako vam sve ovo zvući malo komplikovano. Ipak ovo je jedna od najnovijih tehnologija u svijetu digitalnih tehnologija.

Ne brinite se jer ovaj Priručnik je kreiran kako bi vam pomogao u savladavaju svih područja znanja koja su potrebne da samostalno napravite inteligentnu IoT aplikaciju.

AITI
trening centar

ALDI INICIJATIVA ZA INOVATIVNI TRENING

Panorama b.b. 73 000 Goražde

Bosna i Hercegovina

INTERNET OF THINGS

UVOD U IOT

AITI-IOT-001-180-1

Uvod u Internet of Things

Ključni koncepti i vještine za karijeru u ioT

AITI

Trening centar

Follow us at @UAITLab

Uvod u Internet of Things

Ključni koncepti i prvi koraci u IoT

1
Poglavlje

Vi vjerovatno već znate šta se podrazumjeva pod IoT.

Mnogi članci i blogovi u vezi ioT često započinju sa svojom vlastitom definicijom IoT nakon čega obično izlistaju statistiku i metriku kako će IoT rastieksponencionalnom brzinom. U ovom Priručniku mi ćemo nastojati da se pridržavamo definicije u kojoj pod IoT podrazumjevamo koncept povezivanja bilo kojeg uređaja (pod uvjetom da ima prekidač za uključivanje i isključivanje) na Internet i druge povezane uređaje. IoT je gigantska mreža povezanih stvari i ljudi – u koju su uključeni svi oni koji prikupljaju i dijele podatke o načinu na koji se koriste i o okolišu koji ih okružuje.

Internet of things (IoT) ili „Internet stvari“ obećava da će „stvari“, uključujući potrošačke elektronske uređaje ili kućanske uređaje, poput medicinskih uređaja, frižidera, fotoaparata i senzora, fizički uređaji u poslovnim kancelarijama i u industrijskim pogonima postati sastavni dio Internet okruženja. Ova paradigma otvara vrata novim inovacijama koje će izgraditi novu vrstu interakcije među stvarima i ljudima i omogućuje realizaciju pametnih gradova, infrastrukture i usluga za poboljšanje kvalitete života i korištenja resursa.

IoT kao nova paradigma podržava integraciju, prenos i analitiku podataka koje generiraju pametni uređaji (npr. Senzori). IoT predviđa novi svijet povezanih uređaja i ljudi u kojem je poboljšana kvaliteta života u kojem će upravljanje infrastrukturom u kući, u automobilu, na poslu ili u gradu biti efikasnije, usluge dostupnije i rkonomičnije.

U većini primjene IoT, glavna uloga IoT-a je isporuka vrlo složenih aplikacija utemeljenih na djelovanju u stvarnom vremenu. Za realizaciju punog potencijala IoT paradigme potrebno je uložiti značajan napor na razvoju odgovarajuće arhitekture, otvoriti sisteme koji su obično zatvoreni, osigurati stroge standarde povezane sa privatnošću i etičkim pitanjima koja su uključena u senzibilisanje podataka, te obezbjediti integraciju pametnih uređaja aplikacijama koje će omogućiti prenos, pohranu i obradu podataka te razvoj algoritama za kreiranje uvida ili autonomno djelovanje i upravljanje.

Ovaj Priručnik će Vam pomoći da budete u mogućnosti da:

- Shvatite vještine koje su vam potrebne da biste bili uspješan programer IoT-a
- Odredite koji hardver treba koristiti u vašem IoT projektu
- Odaberite ispravnu tehnologiju umrežavanja za svoj IoT projekt
- Shvatite prednosti korištenja IoT platforme
- Završite svoj prvi IoT projekt, koji možete primjeniti kao rješenje problema iz stvarnog života.

Sretno.

1. Ključni IoT koncepti i vještine

Industrija 4.0 i IoT; Hardver; Umrežavanje (Networking); Razvoj i dizajn aplikacija; Sigurnost; Podaci i AI

Industrija 4.0 i IoT

Mi se trenutno nalazimo usred izuzetno važne transformacije po pitanju načina na koji mi proizvodimo proizvode, a sve zahvaljujući eksponencionalnom rastu digitalizacije ekonomije i društva u cjelini.

Ova transformacija je toliko uvjerljiva i značajna da ga nazivaju Industrija 4.0 u smislu da ona predstavlja prelaz u četvrtu industrijsku revoluciju.

Četvrta industrijska revolucija, četvrta je velika industrijska smjena od 18. stoljeća. Prije nje, bile su još tri:

- Prva u kojoj se za proizvodnju i transport koristi ugalj i para (mehanizacija procesa proizvodnje korištenjem vode za pokretanje mašina i kasnije vodene pare za pokretanje mašina u proizvodnji i transport putem željeznice);
- Druga počinje masovnom primjenom električne energije za pokretanje mašina i razvojem automobile i kamiona za transport;
- Treća, u kojoj se još uvijek djelimično nalazimo, je uslijedila s eksplozijom primjene računara za upravljanje mašinama, poslovnim procesima, upravljanje transportom.

Na prvi pogled, moglo bi se reći da je četvrta industrijska revolucija samo nastavak treće kroz široko usvajanje kompjutera i automatizacije kako bi se osnažili proizvodni procesi sa automatizovanim sistemima, ovaj prelaz zapravo predstavlja puno više.

Razlika je na prvi pogled veoma mala ali je suštinska.

Kada su uvedni kompjuteri u industriji 3.0, oni su napravili poremećaj na tržištu koji je doveo do pojave potpuno novih tehnologija. Prvi računari su imali za cilj da zamjene ljude koji su obavljali poslove računara prilikom računanja kompleksnih matetematičkih operacija. Od tada do danas kompjuteri su zamjenili ljude u obavljanju mnogih poslova (npr. Isplata novca na bankomatima, ili zamjena ljudi prilikom obrade metala na strugovima sa kompjuterski kontrolisanim mašinama). Međutim, sve ove tehnologije zahtjevaju da glavnu riječ u obavljanju poslova ili davanju instrukcija ima čovjek.

Za razliku od industrije 3.0 u kojoj su kompjuteri imali ulogu da provode odluke koje donosi čovjek, u industriji 4.0, uloga tehnologija je proširena i na tu domenu sa ciljem da obavljaju ulogu koju je igrao čovjek – ulogu donošenja odluka.

I upravo je ta funkcija – funkcija donošenja odluka koja je oomogućena radom povezanih računara i uređaja koji komuniciraju jedni sa drugim kako bi u konačnici donijeli odluku bez uključivanja čovjeka - toliko revolucionarna da se slobodno može nazvati novom industrijskom revolucijom.

Osnova nove tehnologije jeste brisanja granice između fizičkog i digitalnog svijeta. Za to je potrebna kombinacija digitalno-fizičkih sistema, inteligentnih uređaja i inteligentnih platformi zasnovanih na *Machine Lerning* koji to omogućavaju. Ovi sistemi mogu fabrike učiniti pametnim, a kroz napredak primjene ove tehnologije (kako sistemi budu imali na raspolaganju više podataka), naše fabrike biće efikasnije i produktivnije.

Na kraju, mreže ovih sistema i mašina koje su digitalno povezane jedna sa drugom rezultiraće u punoj snazi Industrije 4.0 koja će preoblikovati način na koji proizvodimo proizvode na isti način kao što su to učinile parne mašine, električni motori i CNC mašine.

Iz ovog se može zaključiti das u inteligentne I povezane stvari, uređaji I mašine ključna komponenta Industrije 4.0. Zbog toga se smatra da je IoT temelj industrije 4.0 jer je to tehnologija koja bi trebala da obavi funkciju razvoja mreže međusobno povezanih uređaja koji prikupljaju podatke, razmjenjuju informacije i obavljaju zadatke bez direktnog mješanja čovjeka.

Iako je IoT postao jako poularan posljednjih godina, ova tehnologija nije toliko mlada. Njena evolucija traje više od 20 godina, kao i evolucija definicije okvira u kojem se ona kreće.

Pogledajmo kratko kako je to teklo:

1. IoT emergence

Kevin Ashton aslužan je za korištenje pojma "*Internet stvari*" prvi put tokom prezentacije 1999. o upravljanju lancima nabavke. On je vjerovao da je aspekt "stvari" u načinu na koji komuniciramo i živimo u fizičkom svijetu koji nas okružuje potrebno ozbiljno preispitivanje, zbog napretka u računanju, Internetu i brzini generisanja podataka na pametnim uređajima.

U to je vrijeme bio izvršni direktor u MIT-ovom Auto-ID centru, gdje je pridonio proširivanju RFID aplikacija u šire domene, što je osnovalo trenutnu IoT viziju.

Vaš cilj:

Razumjeti ključne koncepte i oblasti u kojima je potrebno razvititi vještine za rad u području Internet of Things

2. Internet of Everything (Internet svega)

Od tada su predstavljene mnoge definicije IoT-a, uključujući definiciju koja se uglavnom usredotočuje na potrebe povezivanja i senzore za subjekte koji su uključeni u tipična IoT okruženja. Dok te definicije odražavaju osnovne zahtjeve IoT-a, nove IoT definicije daju veću vrijednost potrebi sveprisutnim I autonomnim mrežama objekata u kojima integracija identifikacije I usluga ima važnu I neizbježnu ulogu. Na primjer, Internet of Everything (IoE) Cisco koristi za označavanje ljudi, stvari I mjesta koja svoje usluge mogu izložiti drugim subjektima.

3. Industrial IoT

Nazvani Industrijskim internetom, Industrial IoT (IIoT) je još jedan oblik IoT aplikacija koje favoriziraju velike visokotehnološke kompanije. Činjenica da strojevi mogu obavljati određene zadatke poput prikupljanja podataka i komunikacije preciznije od ljudi potaknula je usvajanje IIoTe. Komunikacija stroj-stroj (M2M), analiza velikih podataka i *Machine learning* tehnike glavni su gradivni blokovi kada je u pitanju definicija IIoT-a. Ovi podaci omogućavaju kompanijama brže otkrivanje i rješavanje problema, što rezultira ukupnom uštedom novca i vremena. Na primjer, u proizvodnojkompanijiIIoT se možekoristiti za efikasno praćenje i upravljanje lancima nabavke, obavljanje kontrole i osiguranja kvalitete i smanjenje ukupne potrošnje energije.

IoT se koristi u širokom rasponu industrije: između ostalih, zdravstvu, proizvodnji, automobilskoj industriji, maloprodaji i automatizaciji poslovnih i stambenih zgrada I kuća.

Sada kada smo se upoznali o nadolazećoj četvrtoj industrijskoj revoluciji i ulozi IoT, vrijeme je da vidimo koje su vještine potrebne kako bi mogli razviti karijeru u ovom vrlo uzbudljivom području.

Vrijednost IoT-a prepoznata je iz prikupljanja velikih količina podataka koji se koriste za automatizovano donošenje odluka i poboljšanje operativne efikasnosti. Sa brzinom brzog prihvaćanja IoT-a, potražnja za kvalificiranim programerima IoT-a raste u tandemu, jer IoT transformira način na koji živimo i radimo.

Programeri koji žele maksimalno iskoristiti mogućnosti IoT-a trebali bi njegovati vještine u različitim ključnim tematskim područjima, koje suobrađene u AITI programu obrazovanja u oblasti Internet of Things, a kojeu ključuju:

- Hardver
- Umrežavanje
- Dizajn aplikacije i razvoj aplikacija

- Sigurnost
- Upravljanje podacima, automatizacija i vještačka inteligencija

Hajmo se sada ukratko upoznati sa svakom od ovih oblasti kako bi dobili bolji uvid u to šta podrazumjeva karijera u području Internet of Things.

Hardver 101

U srcu IoT-a su povezani uređaji.

Tu spadaju digitalni uređaji koji se povezuju s drugim uređajima (mašina-mašina) i prvenstveno fizički uređaji koji imaju ugrađenu elektroničku ploču /krug sa senzorom, a koji prenose podatke na određeno odredište - dashboard, platformu za daljinsko nadgledanje ili druge centralne tačke prijema podataka.

Podaci uključuju slike, tekst i druge parametre koji služe za pružanje informacija.

Sa svojim senzorima i svojstvima uređaji uključuju ponešto o hardverskom dizajnu. Međusobna povezanost i cjelovita mrežna konfiguracija podrazumijeva vještine dizajniranja mreže. Obje vrste dizajna mogu koristiti softverski inženjerski dizajn i integrirati se s drugim softverom za formiranje visoko inteligentne mreže uređaja, mašina i sistema, a sve koordinirano radi postizanja ciljeva dizajna i pružanja inteligentnih informacija.

Dizajn uređaja uključuje mogućnost procesa i pohrane podataka. Uređaji mogu koristiti ili mikrokontroler ili detaljniji *System-on-a-Chip* (SoC), koji kombinuje više komponenti poput CPU-a i I / O-uređaja s integriranim krugom.

Uređaji IoT ugrađeni su i moraju biti dizajnirani u skladu s vidljivim karakteristikama planiranih ciljeva dizajna. Te karakteristike uključuju:

- Uslovi okoline
- Vrsta senzora koji će se koristiti
- Količina podataka za genrisanje
- Potrebna snaga, domet i brzina pružena dizajnom uređaja
- Jedinični trošak uređaja i njihov ukupni trošak vlasništva

Dizajn uređaja IoT može se prototipirati korištenjem platformi kao što su Arduino ili računala s pločama poput Raspberry Pi, s prilagođenim tiskanim pločama (printed circuit boards - PCB) razvijenim u kasnijoj fazi.

Za izradu prototipa s ovim platformama potrebne su vještine dizajniranja elektroničkih krugova, kao i programiranje mikrokontrolera i razumijevanje hardverskih komunikacijskih protokola poput serijskog, I2C ili SPI koji se obično koriste za uspostavljanje komunikacije između mikrokontrolera i povezanih senzora i pokretača. Ugrađeni programi često se razvijaju pomoću C ++ ili C, međutim Python i JavaScript postaju sve popularniji za prototipiranje IoT uređaja.

Umrežavanje (Networking)

Umrežavanje je još jedan ključni aspekt IoT-a koji omogućuje uređajima komunikaciju s drugim uređajima kao i komunikaciju s aplikacijama i uslugama koje se izvode u oblaku. Dizajn i upravljanje mrežom ključne su vještine unutar IoT-a, zbog velike količine priključenih uređaja i utjecaja koji odluke o dizajnu mreže mogu imati.

Na primjer, elementi koji se sastoje od mreže (mesh) su mreže predstavljaju dizajn koji se lako može nadograđivatia često se koriste za IoT. Međutim, distribuirana priroda mesh mreža sistav čini složenijim i povećava kašnjenja u protoku podataka (eng. Latency) i snage za svaki od uređaja u mreži.

Uz dizajn mreže, programeri bi trebali imati dobro znanje o mrežnim standardima, protokolima i tehnologijama. Tu se ubrajaju Wi-Fi, niskoenergetski Bluetooth, Zigbee, stanična, RFID tehnologija koja se koristi u potrošačkim aplikacijama i tehnologije široke mreže niske potrošnje (LPWAN) poput LoRa. LPWAN također uključuje SigFox i NB-IoT (uskopojasni IoT) koji nude niže cijene, bežične bežične veze male snage, koje su pogodnije za velike i industrijske IoT aplikacije.

Pored ovih evolucija mrežnih tehnologija, koje predstavljaju više od interneta samo o stvarima, a uopšte o digitalizaciji, postoje i brojne tehnologije povezivanja koje su više povezane sa samim IoT, kao što su:

- **Od Bluetooth i NFC do WiFi i ZigBee**

Primjeri uključuju rješenja za bežično povezivanje kratkog dometa kao što su RFID, NFC, Bluetooth, Wi-Fi i specifični pristupi hrpe vjerojatno manje poznatih zvučnih stvari poput ZigBee, Z-Wave (za kućnu automatizaciju) ili UWB (Ultra Wide-Band)).

Štoviše, kao što je spomenuto, u nekim su vam okolnostima potrebne mobilne mreže ili čak satelitske veze (Iridium project ili za veće stvari StarLink), ali sve zavisi od specifičnosti projekta I komunikcijskih standarda koji će se odabrati.

Tehnologiju na koju trebate obratiti pažnju je ZigBee.

Zigbee je jedino cjelovito LoT rješenje - od mash mreže do univerzalnog jezika koji omogućuje pametnim objektima da rade zajedno. Zigbee povećava izbor i fleksibilnost za korisnike i programere i pruža sigurnost da će proizvodi i usluge djelovati zajedno kroz standardizaciju i testiranje svih slojeva gomile.

ZigBee certificirani proizvodi mogu se međusobno povezivati i komunicirati istim IoT jezikom, a milijuni Zigbee proizvoda već su raspoređeni u pametnim kućama i zgradama. Zigbee je izgrađen s kompatibilnošću unatrag i naprijed.

ZigBee je namjenjen za tržišta kao što su pametne kuće i komercijalne objekte, a karakterišu ga fleksibilna mesh samo-organizacija, ultra niska potrošnja energije i velike biblioteke aplikacija koje developerima stoje na raspolaganju.

Više o ZigBee možete saznati u poglavlju 3.

- **Celularni IoT**

U povezivanju IoT uređaja veliku ulogu igraju mobilne (celularne) mreže.

Očekuje se da će slijedeće godine (2021) biti oko 1,5 milijardi IoT uređaja koji će biti povezani pomoću mobilnih mreža, od čega će jedna četvrtina biti u upotrebljena u automobilskoj industriji.

IoT koristi različite tipove mobilnih mreža kao što su 2G, 3G, 4G, LTE-M, LTE-MTC, NB-LTE-M i NB-IoT.

Posljednje dvije mreže (NB-LTE I NB-IoT) se klasificiraju i u LPWAN tehnologije. Ove mreže uskog pojasa nazivaju “potencijalni je ubojica tehnologija” male snage sa širokom opsegom (LPWA), koje djeluju u nelicenciranom spektru.

Očekuje se da naredne godine skoro 50% celularnih IoT uređaja budu uređaji koji će koristiti NB-IoT. U ovu grupu spadaju i mnogo spominjani 5G.

- **LPWA (N) i šire**

Tehnologija koja će zasigurno omogućiti da IoT uđe na velika vrata jeste LPWAN. Pored mobilnog IoT, postoji nekoliko drugih tehnologija bežične mreže, dizajnirane za Internet stvari. Ovdje se pojavljuju tehnologije širokog područja niske potrošnje (LPWA) i LPWAN (mreže širokog širokog napajanja male snage).

Kao što možda znate mnoge komponente ekosustava internetskih stvari dužeg dometa, poput senzora, zahtijevaju malo energije i ponekad koriste podatke koji se šalju duže vrijeme, ali s dužim intervalima i s relativno niskom brzinom prijenosa. LPWAN, koji je bežični, može ponuditi povezivanje koje je takvim uređajima potrebno dulje vrijeme jer je to i mala snaga. Postoje razne LPWAN platforme / tehnologije, uključujući, na primjer, tehnologiju od stroja do stroja (M2M) Weightless, Ingenu (sa svojom RMPA

tehnologijom za IoT i M2M), francuske tvrtke Sigfox i LoRA / LoRaWan. Kao što je rečeno, ova bežična rješenja za IoT povezivanje djeluju u nelicenciranom spektru, dok mobilni IoT ne.

Dizajn i razvoj aplikacija

Web i mobilne aplikacije pružaju korisnički interfejs za interakciju i korištenje podataka s IoT uređaja.

IoT uređaji, takođ, mogu imati svoja vlastite korisničke interfejse (UIs). Glasovno-bazirani interfejsi i gestikulacijski-bazirani interfejsi dobivaju sve veću pažnju unutar IoT-a, posebno za automatizaciju u kući, dok interfejsi proširene stvarnosti (eng. Agumented Reality – AR) pružaju uzbudljive mogućnosti preklapanja IoT podataka u fizičkom svijetu.

Kao rezultat, UI i UX dizajnerske vještine neke su od trenutno najjačih vještina u IoT-u.

Web i mobilne aplikacije razvijene su koristeći jezike visoke razine, a Java, Swift i Node.js među vodećim su jezicima za razvoj aplikacija IoT.

GPS vještine programiranja (geo-prostorno lociranje) posebno su zahtjevne, jer mnoge IoT aplikacije, uključujući nosiva i pametna vozila, imaju lokaciju.

Programeri bi trebali pratiti nove okvire i setove za programere koje mogu iskoristiti za brzo prototipiranje, kao i IoT platforme koje pružaju infrastrukturu i alate za pomoć u automatizaciji izrade, razmještanja, upravljanja i upravljanja IoT aplikacijama.

Raznovrsnost IoT Aplikacija

Kako će izgledati vasa IoT aplikacija zavisi od područja u kojem razvijate vaš ioT projekat. IoT je sveprisutan zahvaljujući tome što ga je usvojila široka spektar industrija. Svestranost IoT-a čini ga atraktivnom opcijom za veliki broj kompanija, organizacija i vladinih odjela tako da vam možemo samo dati okvirni prikaz u kojim sve industrijama možete razvijati vase IoT aplikacije,

1. Poljoprivreda

Za sadnju u zatvorenom prostoru, IoT stvarnost praćenja i upravljanja mikroklimatskim uvjetima postaje stvarnost, što zauzvrat povećava proizvodnju. Za vanjsku sadnju uređaji koji koriste IoT tehnologiju mogu osjetiti vlagu tla i hranjive tvari u kombinaciji s vremenskim podacima, bolje kontrolirati pametne sustave navodnjavanja i gnojiva. Ako npr. Sustavi za prskanje vode dovode vodu samo kad je to potrebno, na primjer, to sprečava trošenje dragocjenog resursa.

2. Potrošačka upotreba

Za privatnog građanina IoT uređaji u obliku nosivih i pametnih domova olakšavaju život. Nosivi proizvodi pokrivaju dodatke poput Fitbita, pametnih telefona, Apple satova, monitora zdravlja. Ovi uređaji poboljšavaju zabavu, mrežno povezivanje, zdravlje i fitness.

Pametne kuće vode računa o stvarima poput aktiviranja okolišnih kontrola kako bi vam kuća bila vrhunska udobnost kad se vratite kući. Večera za koju je potrebna pećnica ili lonac sa krokodilima može se pokrenuti na daljinu, tako da je hrana spremna kad stignete. Sigurnost je također dostupna i time što potrošač ima mogućnost daljinskog upravljanja uređajima i svjetlima, kao i aktiviranjem pametne brave kako bi u kuću mogao ući odgovarajuće ljude čak i ako nemaju ključ.

3. Zdravstvena zaštita

Prije svega, nosivi IoT uređaji omogućuju bolnicama da prate zdravlje svojih pacijenata kod kuće, smanjujući tako boravak u bolnici, a istovremeno pružaju do trenutnih informacija u stvarnom vremenu koje bi mogle spasiti živote. Pametni kreveti u bolnicama stalno informiraju osoblje o raspoloživosti i time skraćuju vrijeme čekanja za slobodan prostor. Stavljanje IoT senzora na kritičnu opremu znači manje kvarova i veću pouzdanost, što može značiti razliku između života i smrti.

Njega starijih osoba postaje znatno ugodnija za IoT. Osim gore spomenutog praćenja kod kuće u stvarnom vremenu, senzori također mogu utvrditi je li pacijent pao ili pretrpio srčani udar.

4. Osiguranje

Čak će i industrija osiguranja imati koristi od revolucije IoT-a. Osiguravajuće kuće mogu ponuditi svojim osiguranicima popust za IoT nosive uređaje, poput Fitbita. Primjenom praćenja kondicije osiguratelj može ponuditi prilagođene politike i potaknuti zdravije navike, što dugoročno koristi svima, osiguravatelju i kupcima.

5. Proizvodnja

Svijet proizvodnje i industrijske automatizacije drugi je veliki pobjednik u IoT nagradnim igrama. RFID i GPS tehnologija mogu pomoći proizvođaču u praćenju proizvoda od njegovog početka na tvorničkom podu do njegovog postavljanja u odredišnu trgovinu, cijeli lanac opskrbe od početka do kraja. Ovi senzori mogu prikupljati informacije o vremenu putovanja, stanju proizvoda i uvjetima okoline kojima je proizvod bio podvrgnut.

Senzori pričvršćeni na fabričku opremu mogu vam pomoći u prepoznavanju uskih grla u proizvodnoj liniji, smanjujući na taj način izgubljeno vrijeme i otpad. Ostali senzori

montirani na istim tim strojevima također mogu pratiti performanse stroja, predviđajući kada će jedinica trebati održavanje, čime se sprečavaju skupa oštećenja.

6. Maloprodaja

IoT tehnologija mnogo može ponuditi svijetu maloprodaje. Podaci o prodaji na mreži i u trgovini mogu kontrolirati automatizaciju skladišta i robotiku, informacije prikupljene iz IoT senzora. Veliki se dio oslanja na RFID-ove koji su već u širokoj uporabi širom svijeta.

Prostori u trgovačkim centrima su jade stvari; Posao ima tendenciju osciliranja, a pojava internetskih kupovina smanjila je potražnju za postrojenjima od opeke i maltera. No IoT može pomoći u analizi prometa u trgovačkim centrima tako da trgovine smještene u trgovačkim centrima mogu izvršiti potrebna prilagođavanja koja poboljšavaju kupčevo iskustvo kupnje uz smanjenje troškova.

Govoreći o angažmanu kupaca, IoT pomaže trgovcima da ciljaju kupce na temelju prošlih kupovina. Opremljen informacijama koje pruža putem IoT-a, prodavač može izraditi personaliziranu promociju za svoje vjerne kupce, čime eliminira potrebu za skupim promocijama masovnog marketinga koje ne predstavljaju veliku šansu za uspjeh. Veliki dio tih promocija može se provesti putem pametnih telefona korisnika, posebno ako imaju aplikaciju za odgovarajuću trgovinu.

7. Transport

Do ovog trenutka, većina ljudi je čula za napredak koji je postignut kod samovozećih automobila. Ali to je samo jedan zalogaj ogromnog potencijala u području prometa. GPS, koji je, ako mislite na to, još jedan primjer IoT-a, koristi se kako bi se prijevozničkim kompanijama pomoglo da brže i efikasnije kreću rute za teretna vozila te tako ubrzavaju rokove isporuke.

Već je postignut značajan napredak u navigaciji, još jednom aludirajući na GPS telefona ili automobila. No, urbanisti također mogu koristiti te podatke kako bi odredili obrasce prometa, potražnju parkirališnog prostora te izgradnju i održavanje cesta.

Postoji čak i mogućnost da se naprave aplikacije koje mogu spriječiti pokretanje automobila ako vozač pijan.

8. Komunalne usluge / energija

IoT senzori se mogu koristiti za nadgledanje stanja okoliša, kao što su vlaga, temperatura i rasvjeta. Informacije koje pružaju IoT senzori mogu vam pomoći u stvaranju algoritama koji reguliraju potrošnju energije i odgovarajuća prilagođavanja, eliminirajući ljudsku jednadžbu (i priznajmo to, tko od nas nije zaboravio isključiti svjetla u sobi ili isključiti) termostat?).

Pomoću IoT nadzora okoliša tvrtke i privatna prebivališta mogu doživjeti značajne uštede energije, što dugoročno donosi koristi svima, uključujući okoliš!

Podaci prikupljeni Internetom stvari mogu se uvelike upotrijebiti za učinkovitije pokretanje gradskih mreža napajanja, analizirajući faktore poput upotrebe. Također, senzori mogu pomoći bržem utvrđivanju kvarova, čime se povećava vrijeme odziva popravaka posade i smanjuje vrijeme zamračenja.

Sigurnost

Cyber-sigurnost je najvažnija u bilo kojoj raspravi o IoT-u.

IoT uređaji su prilično ranjivi na sigurnosne kompromise. Mnoga kompanije prijavljuju napade na njihove IoT projekte. Ostali su možda napadnuti, a da toga nisu ni svjesni.

Operativna tehnologija - IoT uređaji i njihove mreže - izloženi su velikom sigurnosnom riziku. Međutim, takav se rizik često rješava u mješavini uobičajenih mjera kibernetičke sigurnosti IT odjela.

Ovo možda nije dovoljno.

Organizacije koje koriste IoT trebale bi primjenjivati različite politike za operativnu tehnologiju, odvojene od ostalih mreža unutar organizacije. To bi trebalo uključivati vježbe, reagiranje na incident, planove za oporavak od katastrofe i posebne politike za napade *ransomwarea*.

Sigurnost se mora ugraditi na svakom koraku dizajna IoT sistema, a ne dodavati kao naknadno projektno rješenje/unaprijeđenje.

Kritična pitanja usko povezana sa sigurnošću uključuju etiku podataka, privatnost i odgovornost.

IoT sigurnosna pitanja trebala bi uključivati najmanje:

- Pristup krajnjoj točki (eng. Endpoint access)
- Šifriranje podataka gdje je potrebno
- Odgovarajuća provjera autentičnosti

Kako milijuni novih uređaja svakodnevno ulaze u IoT područje, broj mogućnosti za napade se povećava. IoT uređaji se zlonamjerno koristte za pokretanje distribuiranog uskraćivanja usluge (eng. Distributed Denial of Service - DDoS), kao i za druge teške i štetne napade.

Za sigurnost IoT razvijen je niz preporuka za unaprijeđenje syber sigurnosti IoT sistema kao I okvira za unaprijeđenje sigurnosti kritične IoT infrastrukture.

Zbog tolikog uloga, IoT-ove vještine se visoko smatraju u IoT-u. To uključuje procjenu prijetnje, etičko hakiranje, šifriranje radi osiguranja integriteta podataka, osiguranje mrežne arhitekture i aplikacija, kao i nadzor događaja, evidentiranje aktivnosti i obavještavanje o prijetnjama.

Podaci i AI

Jedna od osnovnih svrha IoT uređaja jeste prikupljanje I razmjena podataka. U tom procesu danas nezamjenjivu ulogu igra vještačka inteligencija.

Zbog toga umjetna inteligencija (AI) sve više postaje sastavni dio IoT mreža.

To je zbog širenja podataka, primjene boljih, prilagođenih, algoritama za rad sa podacima koje prikupljaju IoT uređaji kao i zbog poboljšanja snage i mogućnosti pohrane uređaja.

Svakako ovome doprinosi sve prisutnija primjena *Big Data* koncepta i napredne analitike.

Inteligentna analitika velikih podataka uključuje primjenu kognitivnih tehnika računarstva izvučenih iz procesa vađenja podataka, modeliranja, statistike, primjene *Machine Learning* tehnika AI.

Te se tehnike mogu primijeniti u stvarnom vremenu na senzorske tokove podataka za prediktivnu analizu ili za autonomno donošenje odluka kao odgovor na dolazne podatke, a mogu se primijeniti i na povijesne podatke kako bi se identificirali obrasci ili anomalije u podacima.

Mnogi IoT uređaji generiraju kašnjenje ili vremenski osjetljive podatke, pa je potrebno filtrirati ili odbaciti nevažne podatke. Ključne tehnologije i platforme za analizu podataka na kojima bi IoT programeri trebali razviti vještine uključuju Hadoop, Spark i NoSQL baze podataka.

U ovom priručniku vi se možete upoznati sa osnovama Machine learning tehnika i primjene Vještačke inteligencije kako bi vaši iot projekti imali sposobnost inteligetne primjene u jednoj sveobuhvatnoj IoT aplikaciji.

Obzirom da je napredna analitika, Machine learning i upravljanje podacima izuzetno složena oblast, AITI je razvio poseban kurs koji je u potpunosti posvećen ovoj oblasti (AITI Program obrazovanja u oblasti upravljanjei analiza podataka).

Sada kada smo se upoznali sa osnovnim vještinama koje su vam potrebne da bi razvili inteligentnu IoT aplikaciju, u narednoj sekciji možete saznati više o osnovnoj arhitekturi na kojoj možete izgraditi vaš IoT projekat.

2. IoT arhitektura

Referentna IoT arhitektura; Dva osnovna tipa IoT arhitekture; Najbolje prakse u dizajniranju IoT arhitekture

Referentna IoT arhitektura

Gradivni blokovi IoT-a su senzorni uređaji, daljinsko pozivanje usluga, komunikacijske mreže, i kontekstno svjesna obrada događaja. Sve ove komponente su već dugo prisutne na tržištu. Puno ranije nego što se pojavio termin IoT.

Šta je onda IoT?

IoT objedinjuje sve ove komponente u jednu jedinstvenu distribuiranu mrežu pametnih objekata i ljudi odgovornih za njihovo upravljanje (ako je potrebno) a koji su sposobni za univerzalnu i sveprisutnu međusobnu komunikaciju.

Kada govorimo o distribuiranom okruženju, međusobna povezanost među entitetima je kritični zahtjev, a IoT je dobar primjer. Holistička sistemska arhitektura za IoT mora garantovati besprijekorno rad njegovih komponenti (pouzdanost se smatra najvažnijim faktorom dizajna uvoza u IoT-u) i veza fizičke i virtualne oblasti zajedno. Da bi se to postiglo, potrebno je pažljivo razmatranje u dizajniranju procesa identifikacije i popravke kvarova (pogotovo ako se radi o novim inovacijama u primjeni IoT) i kapaciteta mreže za povećanje i replikaciju (skalabilnost).

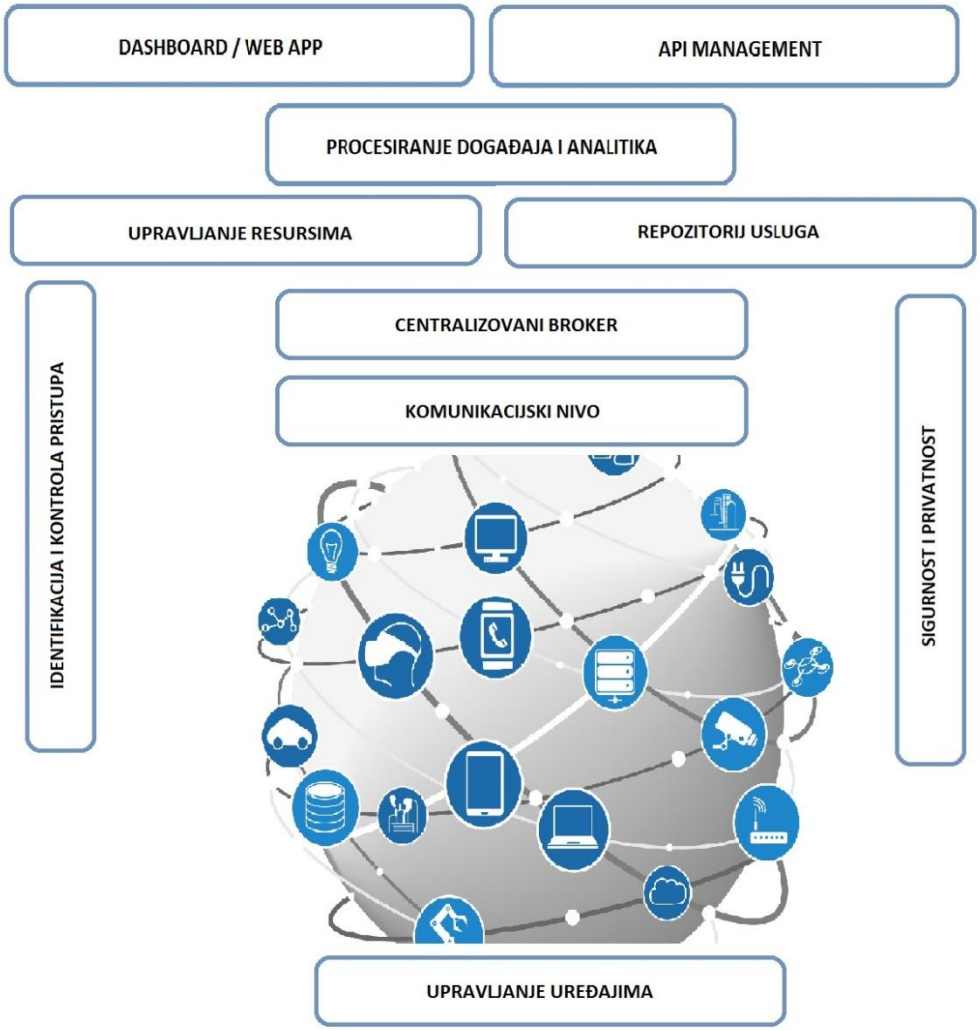
Uz to, imaju mobilnost i dinamična promjena lokacije da postanu sastavni dio IoT sistema sa širokom upotrebom pametnih telefona, najsavremenije arhitekture moraju imati određeni nivo prilagodljivosti da bi pravilno upravljale dinamičkim interakcijama unutar čitavog ekosistema.

Referentne arhitekture i modeli pružaju ptičji pogled čitav temeljni sistem, dakle njihova prednost u odnosu na ostale arhitekture oslanja se na pružanje boljeg i većeg nivoa apstrakcije, što prema tome sakriva specifična ograničenja i detalje provedbe.

U ovom priručniku imaćete priliku da se detaljno upoznate sa arhitekturom IoT projekta koja je ključna u razvoju vaše inteligentne IoT aplikacije.

U ovom uvodnom dijelu je važno da razumijete osnovne komponente arhitekture IoT, ili kako se to još naziva IoT referentna arhitektura. IoT arhitektura fokusira se na razvoj i validaciju integrirane IoT mrežne arhitekture i podrške gradivnim blokovima, s ciljem da se definiše univerzalni pristup razvoju infrastrukture IoT projekata i promovisao sistemski pristup razvoju IoT rješenja, pronalaženju zahtjeva i identifikaciji interesa.

Prikaz: Referentna IoT arhitektura



Predhodna slika šematski prikazuje verziju referentne arhitekture za IoT. Različite servisni i prezentacijski slojevi prikazani su u ovoj arhitekturi. Slojevi usluga uključuju obradu događaja i analitiku, upravljanje resursima i otkrivanje usluga, kao i prikupljanje poruka i Centralizovanog brokera (eng. Enterprise Service Bus -ESB) koji predstavlja usluge izgrađene na vrhu komunikacijskih i fizičkih slojeva.

API upravljanje, što je bitno za definiranje i dijeljenje sistemskih usluga i web-nadzornih ploča (ili ekvivalentnih podataka) pametne aplikacije) za upravljanje i pristup ovim API-jevima, također su uključene u arhitekturu.

Zbog važnosti upravljanja uređajima, sigurnosti i primjene privatnosti u različitim slojevima i mogućnost da jedinstveno identificiraju objekte i kontroliraju njihovu razinu pristupa.

Dva osnovna tipa IoT arhitekture

U principu, u svom radu vi se možete susresti sa dva osnovna tipa IoT arhitekture: Servisna orjentisana arhitektura (eng. Service-oriented architecture – SOA) i API-orjentisane arhitekture.

Pogledajmo šta su njihove osnovne karakteristike

1. IoT SOA-bazirana arhitektura

U IoT-u bi server orijentisana arhitektura (SOA) mogao biti izuzetno privlačna opcija dobavljačima i korisnicima usluga.

SOA osigurava interoperabilnost među heterogenim uređajima. Da biste to bolje razumjeli, razmotrimo generičku SOA koja se sastoji od četiri sloja, s odlikovanim funkcionalnostima kako slijedi:

- Senzorni sloj je integriran s dostupnim hardverskim objektima da se osjeti status stvari
- Mrežni sloj je infrastruktura za podršku između bežičnih ili žičnih veza između ostalog
- Sloj usluge je za kreiranje i upravljanje uslugama koje zahtijevaju korisnici ili aplikacije
- Sloj interfejsa sastoji se od metoda interakcije s korisnicima ili aplikacijama

Generalno, u takvoj je arhitekturi složen sistav podijeljen na podsisteme koji su slabo spojeni i mogu se kasnije ponovo upotrijebiti (modularna karakteristika raspadljivosti), stoga pruža jednostavan način za održavanje čitavog sistema brigom o njegovim pojedinačnim komponentama.

To može osigurati da u u slučaju kvara komponente ostatak sistema (komponente) i dalje može normalno raditi. Ovo je neizmjerna vrijednost za efikasan dizajn IoT aplikacije arhitekture, gdje je pouzdanost najviše značajan parametar.

SOA se intenzivno koristi u WSN (eng. Wireless Sensor Networks) zbog odgovarajućeg nivoa apstrakcije i prednosti koji se odnosi na njegov modularni dizajn. Donoseći ove prednosti IoT-u, SOA može povećati nivo interoperabilnosti i skalabilnosti među objektima u IoT-u.

Štaviše, od korisnika u perspektivi, sve su usluge apstrahirane u uobičajene skupove, čime korisnik korisniku uklanja dodatnu složenost bave se različitim slojevima i protokolima. Uz to, sposobnost izgradnje raznolikih i složenih usluge sastavljanjem različitih funkcija sustava (tj. modularne kompozibilnosti) putem usluge kompozicija odgovara heterogenoj prirodi IoT-a, gdje je za obavljanje svakog zadatka potreban niz servisni pozivi na sve različite cjeline raspoređeni na više lokacija .

2. API orjentisana arhitektura

API (eng. Application Programing Interface) je termin u programiranju kojim se naziva set definicija subrutina, protokola i alata za razvoj softvera i aplikacija. Jednostavno rečeno, API je jedna vrsta interfejsa koji ima set funkcija koje omogućavaju programerima da pristupe specifičnim osobimama podataka u aplikaciji, bazi podataka ili drugim servisima. Za ovaj kurs je posebno važno da znamo da Web API, kako to ime I sugeriše je API kojem se može pristupiti korištenjem HTTP protokola. API je koncepept prije nego tehnologija koji nam pomaže da programiramo pristup čitanju i zapisivanju podataka u aplikaciji.

Konvencionalni pristupi za razvoj rješenja usmjerenih na usluge koriste SOAP (eng. Simple Object Access Protocol) i udaljeni način poziva (Remote Method Invocation - RMI) kao sredstvo za opis, otkrivanje i pozivanje usluga.

Međutim zbog prekomjernih troškova i složenost koju nameću ove tehnike, Web API-jevi i reprezentativni državni prijenos (Representational State Transfer - REST) se sve više koriste kao metode koje se temelje na obećavajućim alternativnim rješenjima. Potrebni resursi kreću se od širina opsega mreže do računarskog i memorijskog kapaciteta, a pokreće ih “zahtjev-odgovor” transformacije podataka redovito se događaju tokom korištenja senzora.

Lagani formati za razmjenu podataka poput JSON (eng. Java Script Object Notation) može smanjiti gore navedene troškove, posebno za pametne uređaje i senzore s ograničenim ograničenjem količina resursa zamjenom velikih XML datoteka koje se koriste za opisivanje usluga.

To pomaže u korištenjukomunikacijski kanal i efikasniju obradu snage uređaja.

Isto tako, izrada API-ja za IoT aplikacije pomaže davatelju usluga privući više kupaca usredotočujući se na funkcionalnost njihovih proizvoda, a ne na prezentaciju. Uz to je i lakše kako bi se omogućila multitenancy sigurnosnim značajkama modernih Web API-ja, koji zaista sposobni su potaknuti izložbu i komercijalizaciju usluga organizacije. To također pruža efikasne alati za praćenje usluga i cijene u odnosu na prethodne usluge orijentirane na usluge.

Novi pristupi za definiranje i dijeljenje usluga u distribuiranoj i višeagentno okruženje poput IoT-a može smanjiti sofisticiranost otkrivanja usluge u ciklusu razvoja aplikacija i umanjiti režijske troškove servisnih poziva u vrijeme izvođenja.

Za prelazak sa platforme za pružanje usluga (SDP) na platforme temeljene na webu, savjetuje se programerima i poslovnim menadžerima da se usredotoče na razvoj i dijeljenju API-ja iz rane faze životnog ciklusa razvoja aplikacija, tako da na kraju, pravilnim izlaganjem podataka drugim programerima i krajnjim korisnicima, okruženje je otvorenih podataka stvoreno koje olakšava zajedničko prikupljanje podataka, dijeljenje i ažuriranje.

Najbolje prakse u dizajniranju IoT arhitekture

Korisni prototipi IoT mogu se graditi iz različitih vizuelnih i detaljnih alata i predstavljaju značajnu ulogu u prikazivanju vizije i obećanja o uvođenju IoT-a koje planirate vašim projektom.

Nakon što uradite prototip, vrijeme je da se posvetite razvoju cjelovitog projekta. Tada će vaš prvi korak biti da dizajnirate IoT arhitekturu.

Kada za to dođe vrijeme tada morate uzeti u obzir nove aspekte koji nisu bili potrebni u prvobitnoj konceptualnoj fazi (prototip). Vaša arhitektura sistema mora biti dizajnirana unaprijed s tim na umu, ili će vaš projekt zastati prije nego što dođe do proizvodnje, ostavljajući vašu organizaciju ranjivijim konkurentima.

Kako bi vam pomogli da izbjegnete prave neugodnosti u procesu razvoja IoT projekta izdvojili smo za vas nekoliko najboljih praksi prilikom dizajniranja IoT arhitekture za industrijsku potrebu.

1. Planirajte IoT arhitekturu za model podataka koji će razvijati

Svaka IoT aplikacija ima model podataka koji uključuje podatke sa samih uređaja, kao i podatke koje generira korisnik i podatke iz vanjskih sistema. Model podataka mora podržavati slučajeve upotrebe za koje je sistav dizajniran.

Modeliranje ovih podataka i omogućavanje da se model podataka s vremenom razvija elegantno su oba područja koja zahtijevaju veliku pažnju u fazi dizajna. Modelirajte sve od algoritama koji prate istoriju podataka. To vam omogućuje ne samo čuvanje podataka o vremenskim serijama, već i razvoj šeme i drugih podataka tokom životnog vijeka ssistema. Spremanje podataka vremenske serije zasnovano na API-ju presudno je za pravilan rad IoT sistema “Enterprise-grade”. Modelirajte elemente podataka kao i pridružene metapodatke kako biste osigurali bogat, kontekstualiziran grafikon za algoritme koji će se koristiti za obradu podataka u informacije.

2. Započnite od kraja (krajnjeg korisnika)

Većina IoT sistema namijenjena je korištenju od strane korisnika koji možda nije zaposlenik firme koja izrađuje sistem. Korisnički interfejs može biti mobilna ili internetska aplikacija, kao i glasovno ili podatkovno vođeni interfes koji se koristi putem podataka na savim drugoj aplikaciji. Postoji nekoliko uobičajenih elemenata koje bi trebalo uzeti u obzir za krajnje korisnički interfejs bilo koje IoT aplikacije.

- Autentifikacija i autorizacija korisnika
- Demo prodaja u odnosu na proizvodnju pojedinačno nasuprot slučajevima korporativne upotrebe (uključujući prelaze)
- Implementacija, interakcija i vizualizacija mogućnosti korisničke priče (uključujući izvještaje)
- Mehanizam notifikacije stanja upozorenja
- Korisnički generirani / isporučeni podaci

Unutar svake određene vrste interfejsa postoje i druge dimenzije koje je potrebno uzeti u obzir. Neiscrpan popis uključuje:

- Mobilni - distribucija i periodična ažuriranja; Minimalno podržane verzije OS-a
- Web - podrška na nivou pregledača; Vrijeme učitavanja stranice
- Enterprise Connectors - Mehanizmi provjere identiteta, Konfiguracija internetskih mreža, Formati podataka
- Glas - struktura naredbe / upita; Podrška za uređaje (Alexa, Siri, Cortana, itd.)

3. Naučite osnove povjerljive komunikacije

Profesionalni/poslovni IoT sistemi imaju svoje temelje u povjerenju. Na svaku vezu potrebno je s pouzdanjem odgovoriti na sljedeća 3 pitanja na svakom nivou komunikacije:

- Da li uređaj komunicira sa sistemom onako kako bi trebalo biti?
- Je li uređaj zaista onaj za koga tvrdi da je?
- Može li sistem potvrditi da uređaj nije ugrožen?

Na njih se može odgovoriti samo u proizvodnji kada se pravi dizajn upotrebljava od samog početka. Zato bi trebalo da u razvoju arhitekture obratite pažnju na slijedeće:

- **Da server validira uređaj**

Preporuka najbolje prakse je da uređaj potvrdi server putem komunikacije pomoću TLS-a. I HTTP i MQTT protokoli podržavaju TLS. Za naslijeđene protokole koji se ne preslikavaju u HTTP ili MQTT koriste se drugi mehanizmi.

- **Da server potvrdi uređaj**

U većini IoT topologija, uređaj započinje komunikaciju s serverom. U drugim topologijama, i uređaj i poslužitelj komuniciraju s pouzdanim posrednikom, koji prenose komunikaciju između njih. U rijetkim slučajevima, server započinje komunikaciju s uređajem.
Izazovi su tehnika za potvrđivanje s visokim stupnjem pouzdanosti da je vaš komunikacijski partner onaj za koga tvrde.

Preporuka najbolje prakse za IoT aplikacije je da server pokrene uređaj. U idealnom svijetu, uređaj bi u svom hardverskom dizajnu imao pouzdan računski modul (TCM) koji bi unutar njega imao jedinstveni privatni ključ za šifriranje. Ovaj izazov zajedno s drugim ulazima proslijedit će se TCM-u radi dobivanja odgovora na izazov. Pomoću ove tehnike poslužitelji mogu otkriti da li netko lažno predstavlja uređaj (kompromitiranim vjerodajnicama) ili je uređaj oštećen nekim oblikom zlonamjernog softvera.

- **Da tokeni imaju rok verifikacije**

Istekli tokeni tehnika je tehnika u kojoj uređaj pristupa usluzi pružanja usluga kako bi nabavio token i zatim token koristi za komunikaciju s IoT aplikacijom na poslužitelju. Ova tehnika nije robusna kao mehanizam punog izazova, ali ima prednost pružanja vremenskog okvira za podvige u slučaju da žeton bude ugrožen.

- **Da se cerfitikati mogu dijeliti**

Druga uobičajena tehnika je generiranje zajedničkog certifikata koji se učitava na uređaj i poslužitelj. Ova tehnika može dobro funkcionirati, ali uvodi probleme oko upravljanja životnim ciklusom certifikata.

- **Da postoji mrežna autentifikacija**

Često postoje zahtjevi za potvrdom identiteta s određenim komunikacijskim kanalom kako bi se mogla uspostaviti internetska veza. U ćelijskom svijetu ovo obično diktira mrežni dobavljač kojim upravlja ćelijski modul. U WiFi svijetu to obično diktira infrastruktura usmjerivača (WPA2, WEP itd.) I ima različitu podršku ovisno o WiFi modulu. Važno je razumjeti varijacije WiFi okruženja krajnjih kupaca kako bi se osigurala mogućnost mrežne provjere autentičnosti. Na primjer, mnoge kompanije zahtijevaju da se WPA2 Enterprise poveže na njihov WiFi, ali ne podržavaju svi WiFi moduli ovaj standard.

4. Razumjevanje kompleksnosti identiteta

Identitet je fluidan koncept u IoT sistemima. Postoji više pojmova identiteta koji mogu varirati ovisno o vašem referentnom okviru. Što je još važnije, svaka se podvrsta može vremenom mijenjati s utjecajima koji se razilaze po cijelom sistemu.

Pogledajte 7 primjera različitih identiteta koje jedan uređaj može imati u poslovnom IoT sistemu.

- **Identitet komunikacijske mreže** - vrijednost jedinstvenosti za komunikacijski kanal poput MAC adrese za WiFi uređaje i IMEI ili MEID za mobilne uređaje.
- **Proizvodni identitet** - vrijednost jedinstvenosti proizvodnog sistema koji se koristi za praćenje serijskih i neserializiranih dijelova podkomponenata koji su ušli u specifični uređaj određenog uređaja.
- **Identitet kompanije** - vrijednost jedinstvenosti za sistem IT u kompaniji koji koristi softver koji mora znati o uređaju.
- **IoT identitet** - vrijednost jedinstvenosti IoT sistema koji se koristi za povezivanje dolazne komunikacije s određenim uređajem i upućivanje izlaznih naredbi određenom uređaju.
- **Identitet kupca** - kako se korisnik odnosi prema uređaju, koji često nije specifičan za uređaj, već stvar / imovina koju uređaj nadgleda i kontrolira ili lokaciju u nekom procesu.
- **Identitet uređaja** - ono što uređaj zna i može prijaviti IoT sistemu o svom identitetu.
- **Financijski odgovoran identitet subjekta** - stranka koja je na kraju "vlasnik" uređaja i odgovorna za plaćanje bilo kakvih naknada za usluge.

Ovi se identiteti s vremenom često mijenjaju.

Presudno je napraviti mapiranje identiteta na početku projekta i osigurati da širi tim od proizvodnje do poduzeća bude svjestan utjecaja bilo kakvih promjena identiteta. U idealnom slučaju bilo bi preslikavanje 1: 1 između identiteta Manufacturing, Enterprise, IoT i Device, ali to je rijetko slučaj u retro-fit scenarijima ili kada je uključeno više dobavljača.

Postoji najmanje 5 ključnih događaja koji pokreću promjene u barem vrsti identiteta.

- **Kompletna zamjena uređaja** - identitet kupca može ostati isti, ali ostali se identiteti mogu ili ne moraju mijenjati. Ako prethodni uređaj trajno nestane iz upotrebe, onda bi trebao biti označen neaktivnim u svim sustavima, a ako ga je prodao, treba ga premjestiti u popis uređaja za kupce. Povijesni podaci moraju

biti pravilno segmentirani i dozvole postavljene ovisno o određenim uvjetima prodaje.

- **Zamjena potkomponente** - serijski izvršena podkomponenta može se zamijeniti kao dio servisiranja uređaja. Podaci o zamjenskoj komponenti (i to je historija) i onoj koja izlazi iz usluge često se trebaju bilježiti, a zadaci poput resetiranja tajmera za upozorenja o održavanju moraju se obratiti.
- **Prodaja uređaja** - prodaja pametnog motocikla ili drugog proizvoda mijenja identitet kupca, ali identiteti ostalih uređaja se možda neće mijenjati i utječu na povijesti senzora na različite načine, pa čak mogu imati i zakonskih pitanja vezanih uz privatnost podataka za neke zemljopisne i podatkovne vrste.
- **Zamjena komunikacijskog modula** - kada postanu dostupne bolje brzine prijenosa podataka i razmjene SIM kartica, identitet komunikacijske mreže mijenja se, što se ne može razlikovati od kompletne scenarije zamjene uređaja ili programibilnog serijskog broja.

  Programirani serijski brojevi - kada se identitet može programirati na uređaju, što može sadržavati pogreške ili propuste ključnih koraka koji vode do dupliciranih identiteta.

5. Voodite računa o vremenu

Za svaku tačku podataka u IoT sistemu postoji višestruko poimanje vremena. Vrijeme događaja (eng. Event Time), zvano „aktualizirano u“ vremenu, opisuje kada se fizički događaj dogodio. Vrijeme server (eng. Server Time), ili 'stvoreno u to vrijeme', opisuje kada je fizički događaj stigao u IoT sistem.

Mnogi se događaji događaju u domeni bez pouzdanog pristupa referentnom satu. U NTP terminologiji događaji se dešavaju u Stratumu 16, što je nesinkronizirana vremenska zona. Ovisno o topologiji, događaji i njihova nesinkronizirana vremena mogu se prenositi preko mreže s više hmelja prije nego što dođu do sistema s pristupom referentnom satu. Svaka od ovih bodova unosi dvosmislenost u vrijeme događaja, tako da je Vrijeme događaja zapravo raspodjela vjerojatnosti, a ne diskretna točka.

Vremena događaja su složena zbog činjenice da se događaji mogu dogoditi na sistemima bez pouzdanog pristupa referentnom satu. Da bi se omogućila analitika i mašinsko učenje iz stvarnih podataka, mora se na odgovarajući način računati vrijeme. Evo 5 scenarija u kojima se vremenski formati razlikuju za događaje koji se dogode:

- Prije nego što steknete GPS zaključavanje ili referentno vrijeme od mobilne mreže
- Na uređaju koji je povremeno povezan s mrežom.
- Bez poznavanja lokacije uređaja za određivanje pomaka vremenske zone

- U sistemu koji sadrži samo prirast brojača od vremena pokretanja
- Kada se izvor napajanja u stvarnom vremenu ukloni ili zamijeni

Kao najbolja praksa vrijeme bi trebalo biti predstavljeno u ISO8601 formatu od trenutka kada događaj prvi upravlja sistem koji ima pristup referentnom satu. Ako je poznato i kome se vjeruje, pomak vremenske zone događaja treba sačuvati u najvećoj mogućoj mjeri. U predaji podataka između uređaja Stratum 16, upotreba krpelja na satu korisna je tehnika za sinkronizaciju događaja Event Times.

U slučajevima kada uređaj radi privremeno bez pristupa referentnom satu, najbolja praksa je korištenje taktova za sat vremena događaja i zatim primjenjivanje vremenskih oznaka ISO8601 retroaktivno nakon uspostavljanja referentnog sata. To se najčešće događa u slučaju nabavke GPS zaključavanja mnogo kasnije nakon pokretanja.

6. Koristite "keširane" podatke za čuvanje događaja na uređaju

Predmemorirani (eng. Cached data) podaci su međuspremnici događaja koji se mogu zatražiti i prijaviti kasnije. Ova tehnika je kritična za uređaje koji izlaze i izlaze iz područja pokrivanja. Također je najbolja praksa za sve WiFi uređaje, gdje žele zadržati podatke o snimanju, čak i ako je WiFi veza prekinuta.

Uređaji moraju biti sposobni povezati vremensku oznaku sa svakim događajem i odgovarati na zahtjeve za podatke koji su se dogodili između vremena X i vremena Y, prije X sekunde prije Y i prije sekunde te za podatke koji su se dogodili između X sekundi i Y sekundi od kraja of bootcycle Z.

Najbolja je praksa da uređaji drže valjani kružni međuspremnik koji sadrži h vremenskim žicama, oznakama sata i pokretačkim ciklusom događaja. Ako događaji nisu formatirani do prijenosa, potrebno je posebno paziti prilikom pisanja novih verzija firmvera kako bi se osiguralo autentično prikazivanje firmvera koji je bio u reprodukciji u vrijeme događaja.

3. Planiranje IoT projekta

Osnovna pitanja planiranja IoT projekta; IoT projektni plan (Metodologija izrade IoT projekta)

Osnova pitanja planiranja IoT projekta

U planiranju svakog projekta važno je znati postaviti prava pitanja.

Jednom kada se upustite u svoj prvi IoT projekat, vjerojatno ćete proći kroz mnoge scenarije i opcije

IoT je složeno područje i svako pitanje može dovesti do dodatnih pitanja, što rezultira neumoljivim brojem međusobno povezanih izbora.

Ono što je najvažnije, kako osiguravate da je vaš projekt poslovni uspjeh tijekom cijelog životnog ciklusa?

Brzo globalno prihvaćanje osigurava da IoT nastavi eksponencijalno rasti, uz mnoštvo novih projekata u razvoju i pratećih usluga. Da biste dugoročno osigurali pravilno postavljanje, važno je procijeniti svoju IoT strategiju kao i sposobnost da je izvršite. Za kompanije koje napreduju bez provođenja temeljite analize, raspoređivanje IoT-a može dovesti do mnogih komplikacija.

Ovdje je mali izbor kritičnih pitanja koja biste trebali postaviti prije implementacije svog IoT plana, no tijekom razvoja vašeg projekta pojavit će se mnogo više pitanja:

1. **Koje su najbolje mogućnosti povezivanja uređaja: žičeno, WiFi, radio ili mobilno?**

Ako imate žicu ili WiFi, imate li kontrolu nad postavkom u kojoj će uređaj postojati? Znate li koliko će instalacija mrežnog kabliranja ili infrastrukture na svakoj lokaciji povećati troškove vašeg projekta?

Kontrolirate li WiFi? Ako nemate vezu na WiFI, kako ćete osigurati da budete povezani na svakoj lokaciji kad se nešto dogodi na licu mjesta?

Ako se Radio i drugi distribuirate širom svijeta, kako ćete osigurati da se pridržavate lokalnog zakonodavstva vezano za frekvencije, snage odašiljača i odobrenja koja će vam trebati?

Ako je Cellular, u kojoj mjeri možete biti jasni o tome gdje će se uređaji nalaziti i jesu li fiksni ili se kreću? Opće je pravilo: što više globalnih i više područja unose vaši uređaji, više ćete trebati uložiti u planiranje i uređaj.

2. Koliko će me koštati gubljenje veze i prekidi u radu?

Savjetujemo vam da to pažljivo izračunate da li vaš IoT projekat može imati problee sa gubtkom veze ili prekida u radu.

Možda ćete se iznenaditi brzinom kojom brojevi eskaliraju. Na primjer, IoT projekat može povezivati uređaje WiFi mrežom koja može zakazati. Ukoliko koristite dinamične SIM kartice, vjerovatnoća prekida može biti daleko manja.

Što imate više prekida, više biste trebali uložiti u izgradnju i mogućnosti povezivanja. Također biste trebali procijeniti troškove posjeta na održavanju na licu mjesta i učiniti sve što možete da ih smanjite na minimum. Rana ušteda nabave može imati dugoročno negativne rezultate na projektu ako tekući troškovi eskaliraju.

3. Kako treba odrediti i izgraditi uređaje koji će se povezati i ostati povezani, gdje god da su raspoređeni?

Da li potpuno razumijete raspon okruženja u kojima se očekuje da uređaj radi?

Ovo je znanje ključno i ima značajan utjecaj na odabir hardvera i softvera koji ćete donijeti. Koje IoT komponente će te vi razvijati, a koje planirate da nabavite od drugih dobavljača?

Koliko ste spremni potrošiti na hardver uređaja?

Da li će te koristiti komponente ili gotova rješenja za određene aktuatore, senzore, API, analitiku ili izvještavanje?

4. Kako planirate da pružite podršku korisnicima?

Ako imate problema, a bit će ih i nekih, rješenja će biti brža i uspješnija ako možete razgovarati izravno s IoT stručnjacima koji razumiju uređaj i način na koji on može raditi na mreži.

5. Kako planirate skladištenje podataka i kako osigurati da se podaci mogu koristiti za efikasnu analizu i izvještavanje?

Izvještavanje i analiza su suštinska vrijednost koju donosi IoT.

Pomoću IoT vaši korisnici će biti u stanju prikupiti informacije sa svih uređaja i centralno ih pregledati i upravljati njima, kako bi se uštedio ili zaradio, ili pružio neki drugi utjecaj, poput društvenog ili okolišnog.

Vi možete poduzeti analizu troškova i koristi, ali u pravilu imaćete potrebu da donesete odluku između dva izbora: ili izgraditi interni poslužitelj i kapacitet programera ili da zakupitee Cloud usluge i konfigurirajte svoj projekt u skladu s njihovim pravilima.

Vaš je zahtjev možda tako jedinstven da nemate izbora nego zadržati tim programera i izgraditi i upravljati internim hardverskim i analitičkim softverom. Međutim, za većinu su prilagodljiva rješenja skladištenja i analitike na uobičajenom skladištu prikladna za svrhu i daju bolju vrijednost i opseg razmjera. Imajte na umu da će dodatni softver za analizu podataka i softver za upravljanje sigurnosnim uređajima koji kompanije poput IBM Cloud, Microsoft Azure, Google Cloud ili Amazon AWS razvijaju i dalje dodavati usluge; sve dok ste spremni konfigurirati njihova pravila, npr. MQTT (Telemetry Transport u redu za slanje poruka). Na temelju ove napomene, pružatelji usluga oblaka uložili su tisuće sati u projektiranje, izgradnju i testiranje pouzdanosti u širokom rasponu stvarnih scenarija rada. Iako će vam se u početku teško nalaziti pridržavanje nekih pravila dizajna i standarda, a naći ćete se u iskušenju da dizajnirate jednostavnije prilagođeno rješenje, dobro razmislite je li to razumna i skalabilna dugoročna strategija.

6. Kako osigurati primjenu IoT projekta što sigurnije tokom cijelog životnog ciklusa?

Važno je razmotriti implikacije nekoga kako ulazi u vaš sistav prije nego što se to dogodi, te uložiti na pravoj razini. Zagovaramo i pružamo niz naprednih sigurnosnih značajki koje nude novu, pristupačniju zaštitu i ujedno se pridržavaju sigurnosnih zahtjeva pružaoca Cloud usluga. Dok pripremate svoje uređaje i povežete, trebali biste odlučiti gdje je vaša sigurnosna granica i prema tome planirati.

Razmotrite ozbiljan ugovor s stručnjacima za testiranje penetracije trećih strana i uvjerite se da vaš tim želi to potaknuti.

IoT projektni plan

Metodologija koju možete primjeniti kod razvoja IoT projekta je slična razvoju bilo kojeg drugog projekta u oblasti razvoja aplikacija ili drugog poslovnog projekta.

Naravno da pri tome možete koristiti različite tehnike ili alate koji se primjenjuju u agile *Waterfall* projektnom pristupu o čemu možete saznati u drugim AITI kursevima koji su specijalno dizajnirani kako bi vam pomogli da savladate tehnike razvoja vaših projekata.

Naravno, IoT projekti imaju svoje specifičnosti.

Kako bi vam pomogli u ovoj sekciji ćemo vam pokušati naznake kako bi trebao da izgleda razvoj plana IoT projekta.

Prilikom razvoja IoT projekta potrebno je da posebnu pažnju posvetite:

- Definisanju poslovnih ciljeva
- Izboru IoT platform

- Izboru hardvera
- Identifikaciji komumunikacijskih protokola
- Razvoju plana
- Izgradnja I lansiranje IoT projekta.

Prikaz: Proces skiciranja plana IoT projekta

1. Definisanje poslovnih ciljeva

IoT projekat, kao i svaki drugi projekat treba da obezbjedi dodatnu vrijednost ukoliko želimo dag a organizacija podrži.

Bez dodatne vrijednosti svaki projekat je osuđen na propast.

Postoji bezbroj načina da se korištenjem IoT doda značajna vrijednost poslovanju organizacije. Naš je prijedlog da vaš prvi korak u kreiranju IoT projekta bude usmjeren ka identifikaciji jednog ili dva poslovna cilja koji organizacija može postići projektom.

Ovo je važno jer sa manjim brojem poslovnih ciljeva vi brzo možete pokrenuti pilot projekat i pokazati kako IoT može unaprijediti poslovanje. Jedna ili dvije funkcije koju bi obavljao IoT vi možete otvoriti vrata svom projektu. Kasnije, IoT projekat možete unaprijeđivati, dodavati dodatne funkcionalnosti i integrisati dodatna rješenja koja obavljaju dodatne poslovni funkcije.

Vaš IoT projekat može biti usmjeren na jednu od dva poslovna područja:

- **Interne operativne aplikacije (eng. Internal operation Applications)**, u kojoj možete primjeniti IoT kako bi interno poboljšali poslovanje, povećali operativnu efikasnost ili smanjili operativne poslovanje organizacije
- Aplikacije za potrošačku uključenost (eng. Consumer Engagement Application), u kojoj možete unaprijediti korisničko iskustvo ili otvoriti nove izvore prihoda za organizaciju.

Mnoge kompanije smatraju da je efikasnije da se prvo treba usredočiti na unutrašnju primjenu, poput upravljanja zalihama ili aplikacija za nadgledanje. Brzo možete pokrenuti pilot za kako bi pokazali kako rješenje djeluje i pokazati kako projekat donosi dodatnu vrijednost, a zatim se možete pomaći na područja okrenuta prema potrošačima koja i vi identificirali.

Nekoliko opcija koje vaš IoT projekat može uticati na dodatnu vrijednost su:

Koja je tvoja IoT prilika?

- Novi tokovi prihoda
- Rast prodaje
- Bolje korisničko iskustvo
- Ušteda troškova
- Bolje performance radne snage
- Lanac opskrbe i logistika
- Upotreba imovine
- Inovacija.

2. Izbor IoT platforme

U središtu svake IoT implementacije je IoT softverska platforma.

IoT platforma jemozak iza rješenja - tehnologija koja sve spaja zajedno i omogućava vam kako bi razvili i upravljali krajnjim rješenjem u svim sustavima.

Izabrana IoT platforma bit će jedna od vaših ključnih strateških odluka, jer je dugoročnaulaganje na kojem ćete razviti svoje početno rješenje i stvoriti nova rješenja koja mogu utjecati na više područja poslovanja vaše organizacije.

Zbog toga je vrlo važno da odmah na početu planiranja vašeg IoT projekta razmotrite neka od ključnih pitanja u vezi odabira IoT platforme kao što su.

- **Da li će vaša platforma biti otvorena za integracijsku fleksibilnost?**

Važno je da se vaša platforma lako integrira s drugim platformama i tehnologijama, s budućim tehnologijama koje dolaze na tržište, kao i s vašim naslijeđenim sustavima. Izbjegavajte biti zaključan u vlastitom rješenju kako bi vam pomogao da zadržite fleksibilnost i lako se susrećete sve veći zahtjevi za rješenjem.

- **Kako će se vaša platforma razvijati u skladu sa potrebama?**

Trebat ćete platformu koja je visoko skalabilna da udovolji vašim evoluirajućim potrebama, poput dodavanja nove aplikacije, značajke, uređaji, korisnici, lokacije i još mnogo toga.

Budite svjesni toga dok cijene modeli temeljeni na broju povezanih uređaja mogu biti najisplativija rješenja za pilota to se može pretvoriti u najtrofejnije cijene. Platforma također treba omogućiti možete jednostavno povećati ili smanjiti svoje potrebe za pohranom, velikom analizom podataka i obrada.

- **Trebate li koristiti alate za brzi razvoj aplikacija?**

Platforma koja omogućuje modularni pristup razvoju aplikacija omogućit će vam brzo stvorite, testirajte i pokrenite nove aplikacije. Unaprijed ugrađeni početni setovi s modularnim templatima, robusnu biblioteku API-ja i testno okruženje koje udovoljavaju trenutnim I buduće potrebe su ključne.

- **Trebate li koristiti hibridne mogućnosti – Edge I računanje u Cloud-u?**

Hibridna platforma pružit će vam najbolje iz oba svijeta: usluga na licu mjesta za neposrednost kritični podaci, operativna učinkovitost i lokalizirana analitika za postizanje djelotvornih rezultata u gotovo u stvarnom vremenu. I velike analize podataka i pohrana u oblaku kako bi se pomoglo u ukupnom radu i povećanju poslovni efikasnosti.

- **Kako daljinski planirate upravljati uređajima i hardverom?**

Ključ vašeg IoT rješenja je platforma koja omogućuje daljinsko upravljanje pristupne mogućnosti za upravljanje, rekonfiguracije, ažuriranjai postavljanje kontrola, posebno pri obradi između lokalnih mreže i Cloud-a.

- **Da li će vaša platforma zahtjevati Big Data mogućnosti i vještačku inteligenciju?**

Ukoliko je vaš IoT projekat usmjeren ka jednostavnijim korištenjem mogućnosti IoT, kao što je na primjer automatska regulacija temperature u objektu ili pametno upravljanje rasvjetom, tada vjerovatno vi nećete imati pretjeranu potrebu da vaša IoT platforma ima ugrađene mogućnosti da Big Data ili AI. Ali ako imate namjeru da vaš projekat kreira značajnu dodatnu vrijednost za organizaciju razmislite o ovim opcijama.

Za kreiranje značajnog utjecaja na poslovanje, IoT platforma mora biti u mogućnosti da efikasno upravlja velikim količinama podataka kao I za njihovu analitiku, a vaši uređaji bi trebali biti u mogućnosti da generišu velike količine podataka, kao I da na osnovu njih obavljaju određene operacije. Da bi se iz te velike količine podataka mogla izvući vrijednost, važno da ja vaša IoT platform ima ugrađene funkcije vještačke inteligencije, Machine learning algoritme I algoritme napredne analitike.

- **Privatnost i sigurnost**

Sigurnost je vitalni dio svakog IoT rješenja. Na početku je vrlo važno da obezbjedite upravljanje enkripcijom podataka od početka do kraja u mirovanju i u pokretu za i provjere autentičnosti korisnika i uređaja. Pobrinite se da cijeli rješenje uključuje robusnu sigurnosnu arhitekturu s ulogom i upravljanje pristupom, sigurnost krajnje točke i sigurno transakcije između uređaja, aplikacija i s Cloud-om.

- **Upravljanje okidačem i akcijama**

Vaša IoT platforma trebala bi podsticati uključenost korištenjem okidača baziranih na pravilima (eng. Rule-based) koji omogućuju "pametne" akcije.

Pravila koja definišete trebaju se moći nositi s stvaranjem logikeizjava "ako-onda" s više vrsta objekata I kombinacija upita.

3. Odabir hardvera i uređaja

IoT hardver široka je kategorija, s nekoliko aplikacija uređaja, u rasponu od korisnika

uređaji, poput nosivih, na senzore koji nadziru gotovo sve.

Postoji širok raspon izvanrežnih uređaja koji se mogu odgovoriti na potrebe većine IoT aplikacija. U narednom poglavlju biće puno više riječi o IoT hardveru I senzorima koji će moći zadovoljiti širok spektar funkcija vaših projekata I koji se relativno jednostavno mogu nabaviti na tržištu.

Ako funkcionalnost koja vam je potrebna nije lako dostupna, postoje proizvođači originalnih dizajna (ODM-ovi) koji mogu izgraditi prilagođeni uređaj koji odgovara vašim potrebama. Proizvođači hardvera trebali bi biti voljni surađivati s vama kako biste

definirali zahtjeve koji će postaviti vaš softver i komunikacijski protokoli kompatibilni unutar uređaja.

Novi hardverski uređaji od mnogih dobavljača izlaze na tržište svakodnevno, zato je vrlo bitno da u fazi planiranja vašeg projekta ponovo provjerite koji su uređaji dostupni kako bi što bolje planirali vaš projekat.

4. Identifikacija komunikacijskih protokola

Komunikacijski protokol povezuje vaše uređaje međusobno kao i na vašu IoT platformu. Vaše rješenje može zahtijevaju više protokola, pa ćete to htjeti osigurajte da vam IoT platforma bude fleksibilna, s kojom se može integrirati nekoliko njih.

Prikaz: Komunikacijski protokoli u zavisnosti od potreba za pojasom i opsegom

Komunikacijski protokoli temelje se na rasponu zahtjeva, koji mogu obuhvaćati:

- **Zahtjevi za širinu pojasa / upotrebe podataka** - količina protoka podataka po uređaju
- **Geografski raspon** - od malog zatvorenog prostora do velikog vanjskog prostora
- **Sigurnost / pristup** - javni ili privatni pristup mreži
- **Izbor uređaja** - različiti uređaji rade preko različitih komunikacijskih protokola
- **Učestalost** - uvijek uključena ili povremena dostupnost

Količina podataka koja vam treba, učestalost koja vam je potrebna i kolika će vam udaljenost pomoći su parametri koji će vam biti potrebni da odredite svoju komunikacijsku tehnologiju.

Na primjer, ako želite čitati brojilo jednom mjesečno da biste generisali račun za korisnika, to je mali iznos podataka u širokom vremenskom intervalu i na širokom geografskom području, LPWAN vam može pomoći da senzore povežete na internet sa velikim uštedama u troškovima. LPWAN-ovi su efiksni za projekte u industriji, poljoprivreda, aplikacijama za pametne gradove ili zgrade.

Suprotno tome, ako želite znati promet prometa kroz vašu maloprodajnu trgovinu, kako biste dobijali obavijesti o plasmanu proizvoda i pokretanju obavijesti u stvarnom vremenu, mobilne mreže, Bluetooth ili Wi-Fi bi dobro funkcionirao.

5. Izgradnja i lansiranje

Ovaj priručnik je razvijen kako bi vam pomogao da razvijete vašu prvu komercijalnu IoT aplikaciju.

Naravno, prvi korak u izgradnji vaše aplikacije počinje sa fazom planiranja. Nakon što ste utvrdili ciljeve vaše aplikacije, definisali neophodnu opremu I komunikacijske protokole na red dolazi da napravite plan kako razviti I lansirati vaš IoT projekat.

U ovoj fazi vi morate donijeti niz odluka koje ćete morati donijeti kako biste odredili najbolje način za izgradnju i implementaciju vašeg IoT rješenja. Evo pet razloga za razmišljanje.

- **Model implementacije**

Jedna od vaših ključnih odluka je kako implementirati svoju IoT platformu - u fizičkom prostor, u oblaku, ili putem hibridnog modela.

Postoje prednosti svakog pristupa.

Velik dio odluke zavisi i o vrsti podataka koju trebate pohraniti i o odnosu vaše organizacije korištenju Cloud-a. Neki od razloga za razmatranje raspoređivanja u postrojenju su u rasponu propisa, sigurnosnih pitanja, pitanja povezivanja i brzine.

Mi snažno podržavamo korištenje Cloud Servisa, a saznaćete i zašto.

Mnoge kompanije preferiraju rješenje u Cloud-u, jer mogu implementirati brže i uz niže troškove razvoja i održavanja, i imati agilnija rješenja, skalabilna platforma koja im omogućuje pokretanje malih i dodavanje ili oduzimanje novih uređaja i tokova podataka po potrebi. Neke kompanije preferiraju hibridni model zbog ograničenja koji radi u isključivo posvećenom ili javnom okruženju.

Hibridni pristup nudi prednosti, poput poboljšane sigurnosti, istodobno iskorištavajući prednosti troškova i skalabilnosti koje donosi Cloud.

- **Resursi za razvoj**

Za razvoj vaše aplikacije važno je da unaprijed odlučiite da li će te koristiti interne razvojne resurse ili ćete koristiti vanjske resure za razvoj vašeg rješenja? Neki vanjski razvojni partneri radit će s vašim internim timom, omogućujući vam da koristite hibridni razvojni pristup.

- **Hardver**

Postoji niz razmatranja koja treba uzeti u obzir kada odabir hardvera, iz prilagođenih razvojnih zahtjeva na okolišne uvjete. Ukoliko koristite hardver koji je lako nabaviti to će vam znatno ubrzati process razvoja aplikacije u odnosu na hardver koji nije lako dostupan I za koji je potrebno dag a namjenski naručite od ODM koji vam može izraditi prilagođenog uređaja.

- **Strategija lansiranja**

Treba li se lansirati s ograničenim pilotom ili uvesti svoje rješenje na nivou cijele organizacije? Već ranije smo dali naznaku da je efikasnije da se u projekat udje sa pilot fazom koja je fokusirana na jedan ili dva zadatka iz kojeg se kasnije može razvijati kompletan projekat.

Ovo vam daje prilika za brzo pokretanje i brzo demonstriranje uspjeh. Tada možete razmotriti dodavanje dodatnih funkcionalnost ili pokretanje u cijeloj organizaciji.

- **Logistika lokacije**

Tokom faze planiranja, važno je posvetiti pažnju na logistiku lokacije povezanu s montažom opreme. Postoje li problemi okoline koji bi trebali biti razmatrani? Postojeći materijali ili oprema koji bi to trebali biti riješiti? Postoje li faktori zaposlenika ili kupca koje treba uzeti u obzir?

6. “Prodaja” plana

Vi ste razradili svoj plan i vrijeme je da ga prezentirate ključnim stakeholderima koji učestvuju u procesu donošenja vrlo važne odluke – odobravanje plana.

Nekada su ključni stakeholder uži krug osoba koje su direktno zainteresovane za projekat. U drugom, puno vjerovatnijem slučaju, vi svoj plan treba da predstavite ključnim osobama u vašoj organizaciji; vašim eksternim klijentima; ili možda korisnicima.

U svakom slučaju ljudima koji odlučuju hoće li se vaš san pretvori u realnost.

Na sreću vi ste se dobro pripremii za ovu ključu fazu, napornim radom na predhodnih pet tačaka. Sada, u ovom finalnom momentu važno je da mislite iznad kratkoročnih poslovnih ciljeva I vaših tehničkih rješenja.

Sada je potrebo da razmišljate strateški I da prodate svoj san.

Evo nekoliko savjeta.

- Dajte vašem projektu stratešku dimenziju

Pokažite kako IoT ulaganje ispunjava strateške ciljeve imajući na umu da su ciljevi vrlo vjerovatno će se razviti s vremenom. Fokusiranjem na strateške poslovne zahtjeve koje vaše IoT rješenje može dostići vi možete kreirati jasniju sliku zašto je vaše rješenje potrebno iidealno za organizaciju.

- Komunicirajte poslovne rezultate

Neka vaš prioritet bude da jasno pokažete poslovne rezultate koje vaše IoT rješenje želi postići.

Može li vaše IoT rješenje povećati prodaju, uštedjeti novac, poboljšati efikasnost, utjecati na vašeodnosi s kupcima?

- Istaknite faktore uspjeha

Kako ćete mjeriti uspjeh? Je li to trošak ili ušteda vremena? Privlačenje novih kupaca?

Kompanije često rade ograničen pilot pilot projekt, a nakon što postignu svoje ciljeve, implementirat će rješenje u cijeloj organizaciji.

- Pokažite širu vrijednost za organizaciju

Vaše IoT rješenje može utjecati na cijelo poslovanje organizacije - ne samo jedan ili dva odjela. Dokažite kako vaše IoT rješenje dodaje vrijednost u vašoj organizaciji.

- Dajte akcenat na transformaciju

Komunicirajte kako vaše IoT rješenje može olakšati poslovnu transformaciju. Koja će novi biznisi moći biti ppodržani sa vašim rješenjem? Kako će se modernizirati operacije ili redefinirati ponudu proizvoda?

- Istaknite buduće mogućnosti

Pomozite stakeholderima da shvate da je predloženo rješenje tek početak.

Prodajte viziju. Dajte im da vide kako platforma može s vremenom evoluirati i utjecati na njihovo poslovanje na svim područjima. Navedite buduće primjere i područja koja će stvoriti nove tokove prihoda.

Mislimo da je ovo dovoljno inspirativno, da možemo krenuti dalje – I baciti se na posao razvoja IoT projekta.

Hardver

Povezani uređaji su centralna tačka IoT

AITI

Skill Accelerator

Follow us at @UAITLab

Hardver

Povezani uređaji su centralna tačka IoT

Početkom 20 stoljeća nafta je bila glavni motor do tada neviđenog progresa i napredka širom svijeta. Sto godina kasnije nafti se bliži kraj (kako zbog ograničenih resursa tako i zvog negativnog uticaja na okoliš) mjesto ključnog resursa na kojem se zasniva razvoj sve više preuzimaju podaci koji su glavni motor četvrte industrijske revolucija (Industrija 4.0).

U predhodnom poglavlju imali ste prilike kako bi napravili dobru strategiju. I kao što ste mogli primjetiti, korištenje ovih alata skoro pa bezvrijedno bez odgovarajućih, tačnih i relevantnih podataka.

Kako bi bili u mogućnosti da skoristite puni potencijal podataka u ovom poglavlju su obrađene teme koje će vam pomoći da usvojite znanja iz oblasti poslovnog obavještanja (Business Intelligence) čija primjena doprinosi boljem, bržem i efikasnijem donošenju odluka, te će steći vještine rada sa podacima u softverskim platformama za provođenje analitike podataka u poslovne svrhe.

U ovom poglavlju vi će te se moći upoznati sa:

- Osnovama pristupa poslovnog obavlještavanja i novim pristupima korištenja poslovnih podataka u procesu donošenja odluka u organizaciji;
- Osnovama rada sa podacima kako bi mogli iskoristiti njihov puni potencijal za primjenu poslovne analike u upravljačkim procesima;
- Mogućnostima koje nude softverkse platfome Tableau i Power BI, dvije trenutno najbolje softverske platforme za poslovnu analitiku i Business intelligence za mala i srednja preduzeća/organizacije.

Znanje sa kom se možete upoznati u ovom poglavlju sigurno će vam olakšati napore na razvoju vaših strateških ideja. Međutim, oni vam takođe mogu biti od izuzetne koristi kada budete razvijali vaše prijedloge projekata putem vi vaše strateške ideje razrađujete u detaljne planove akcije.

Poslovna analitika u doba podataka postaje sve važniji alat koji se primjenjuje u poslovanju, zato ne gubimo vrijeme i krenimo da se upoznamo sa ovom jako zanimljivom temom.

1. Osnove IoT hardvera & uređaja

IoT hardver; IoT senzori

IoT Hardver

IoT hardver kritična je komponenta cjeloukupnog IoT rješenja. U vašim nastojanjima da razvijete IoT rješenje ključno je da shvatite kako kako pametni uređaj prikuplja, obrađuje skladišti I koristiti podatke kako bi obavio akcije koje su predviđene vašim IoT projektom.

Hardverske mogućnosti

Kao što smo ustanovili u prethodnom poglavlju, senzori / uređaji su kritični dio Intereta stvari. Njihova funkcija je da služe kao 'osjetila' sistema i kao sredstvo za interakciju sa svijetom.

Iako niti jedno cjelovito IoT rješenje ne može biti izgrađeno bez nekog hardvera, senzora / uređaja, oni su ponekad podcijenjen aspekt IoT sistema. Izbori koje donosite u vezi vašeg hardvera imaju ključan uticaj na to kako će vaš projekat funkcionisati, od toga koje podatke I koliko brzo će prikupljati, do kapaciteta za povezivanje, analitike koju može obavljati I interakcije koje može ostvariti sa krajnjim korisnicima.

Previše je senzora / uređaja koji vi u svojim projektima možete koristiti da bi se ovde mogoa dati iscrpan popis.. Konačno, odluke koje donesete na hardveru proizlaze direktno iz potreba specifične aplikaciju koju vi planirate razviti.

Vi možete istraživati koje sve opcije senzora / uređaja postoje kako bi razvili svoj projekat, a da vi u tome bili efikasni, važno je da razumijete neke osnovne faktore koje bi trebali uzeti u obzir prilikom razmatranja hardverskih mogućnosti vašeg projekta.

Kao prvo, razmislite o napajanju.

Jedno od prvih razmatranja jesu li senzori / uređaji koje će te koristiti imat raspoloživo napajanje energijom. Ako dizajnirate, recimo, pametnu pametu poljoprivrednu aplikaciju, sa stotinama senzora koji se postavljaju širom velikog ruralnog područja, morat ćete se osloniti na baterije. Ako se vaša aplikacija nalazi u zgradi i uključuje samo nekoliko uređaja, napajanje možda nije problem.

Razlog tome što je ovo jedno od prvih razloga je taj što je to direktno prevodi u koliko možete učiniti sa senzorom / uređajem. Ako se vaš hardver se napaja iz baterije, vi želite da traje dugo - nadamo se godina (kao što ćemo opisati u sljedećem odjeljku,

zamjena I upravljanje baterijama će biti zadatak koji će se nalaziti visoko na ljestvici vaši operativnnih prioriteta.

No, da biste došli do višemjesečnog ili višegodišnjeg trajanja baterije, uređaj ne može biti stalno aktivan. Operacije koje troše puno energije, poput upotrebe GPS ili slanje i primanje poruka preko mreže mora biti dobro planirano.

Da biste dobili dobru informaciju od GPS-a, uređaj mora „slušati“ signale sa najmanje 4 GPS satelita koji su u orbiti. U zavisnosti od terena koji može blokirati prijem GPS signala prijem podataka sa GPS može trajati 30 sekundi, 60 sekundi ili više. Sve to vrijeme vrijeme je da GPS jedinica isprazni dragocjenu bateriju.

Isto vrijedi i za povezivanje. Da biste primali poruke preko mreže, senzori / uređaji moraju biti u režimu „slušanja“, a to znači pražnjenje baterije.

Zato je važno da dobro osmislite kada je potrebno da se vaši uređaji aktivniraju. Postoje li situacije u kojima je dovoljno da se uređaj sam uključi I pošalje poruku, poput aktiviranja alarma?

Četri gradivna bloka IoT hardvera

Odluke o hardveru utječu na cijenu vašeg IoT projekta, korisničko iskustvo, mogućnosti aplikacije i još više.

Često se dešava da osobe koje su zadužene za upravljanje razvojem IoT projekta imaju slabo iskustvo u vezi upravljanja IoT hardverom, ali to i da puno bolje razumiju kako funkconiše softver koji pokreće IoT platform.

Zbog toga je važno da razumijete hardver kako bi bolje razumjeli kako pametni uređaj prikuplja, obrađuje i komunicira podatke sa krajnjim korisnicima.

Upravljanje hardverskim proizvodima zahtijeva vrlo različite vještine od upravljanja softverom. To je jedan od razloga zašto gradnja IoT proizvoda može biti vrlo zastrašujuća za nove IoT proizvode.

Kako bi vam pomogli da bolje razumijete ovo područje, vjerujemo da je korisno da istražite četri ključna područja koje predstavljaju gradivne blokove IoT hardvera.

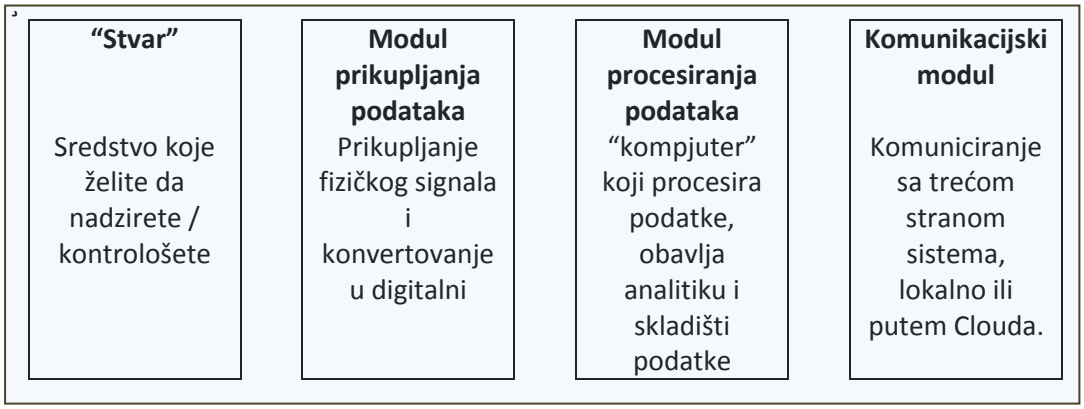
1. Stvari

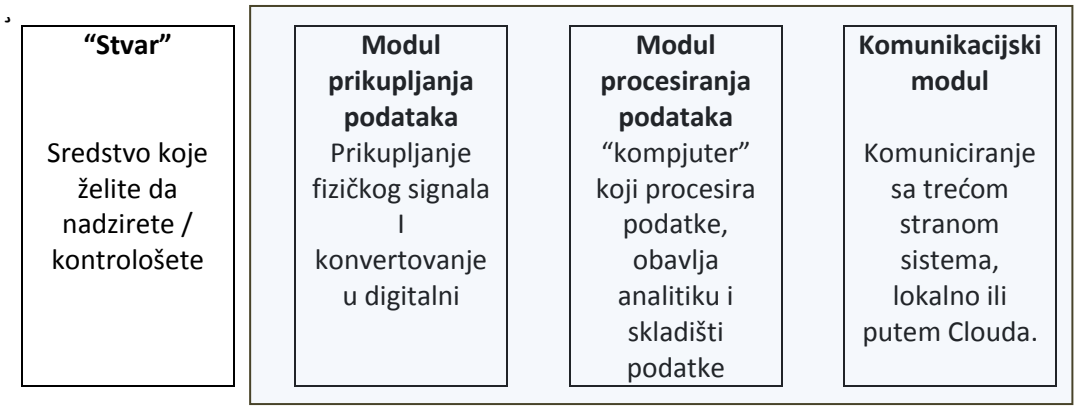
U IoT pod “stvari” (eng. Things) se obično definiše bilo koje fizičko sredstvo koje želite integrisati / nadzirati povezivanjem preko internet.

U mnogim IoT proizvodima "stvar" je potpuno integrirana u pametni uređaj. Na primjer, mislite na proizvode poput pametne pumpe za vodu ili autonomnog vozila. Ti se

proizvodi kontroliraju i nadziru. U ovom slučaju vaš proizvod uključuje sva četiri građevinska bloka u jednom paketu.

Prikaz: Dva osnovna modela “stvari”





Gornji prikaz slikovito opisuje dva modela “stvari” koje vi trebate da uzmete u obzir prilikom planiranja hardvera za vaš projekat. Nekada će biti potrebno da vaša stvar bude samo jako inteligentna I da u sebi ima integrisane module da prikupljanje podataka, njihovog procesiranja I komuniciranja, a ponekad će to biti samo nekao obična stvar koja će nakon što se poveze sa IoT modulima za prikupljanje, procesiranje i komuniciranje podataka.

Razumjevanje ove osnovne podjele možebiti jako korisno. Često će biti slučaj da u industrijskim aplikacijama kompanije imaju postojeću imovinu i žele ih učiniti "pametnim".

Razlog zbog kojeg se ova podjela ističe jeste u tome što je važno da budete svjesni da postoje različiti poslovni modeli koje možete izabrati. Vaša organizacija može odlučiti izgraditi potpuno nove uređaje koji su pametni od samog početka ili možete odlučiti da je vaš prijedlog vrijednosti pružiti način da se postojeće stvari pretvore u pametne stvari, otvarajući vrata onome što se naziva „Brownfield” mogućnosti.

2. Modul za prikupljanje podataka

Modul za prikupljanje podataka fokusiran je na pribavljanje fizičkih signala iz "stvari" i pretvaranje u digitalne signale kojima računalo može upravljati.

Ovo je hardverska komponenta koja uključuje sve senzore koji prihvaćaju signale iz stvarnog svijeta poput temperature, kretanja, svjetla, vibracija itd.

Vrsta i broj senzora koji vam trebaju zavise od vaše aplikacije.

Modul za prikupljanje podataka ipak uključuje više od senzora.

On uključuje potrebni hardver za pretvaranje senzorskog signala u digitalne informacije koje koristi vaša aplikacija. To uključuje kondicioniranje signala, analogno-digitalnu transformaciju, skaliranje i interpretaciju.

Za modul za prikupljanje podataka najvažnija su slijedeća razmatranja:

- Koje fizičke signale treba mjeriti? (tj. koji tip senzora vam je potreban)
- Koliko senzora svake vrste treba IoT projekat?
- Koliko brzo treba izmjeriti signal u stvarnom svijetu? (tj. stopa uzorka)
- Kolika je potrebna tačnost za mjerenje? (tj. razlučivost senzora)

Odgovori na ta pitanja sadržavat će zahtjeve za modulom za prikupljanje podataka i dati vam ideju o tome koliko podataka će vaš uređaj proizvesti.

3. Modul za obradu podataka

Treći gradivni blok IoT hardvera je modul za obradu podataka. Ovo je "računalo" koje obrađuje podatke, obavlja lokalnu analizu, pohranjuje podatke lokalno i na rubu obavlja bilo koje druge računalne operacije.

Prilikom planiranja potreba modula za obradu podataka važno je da razumijete opći cilj proizvoda i postaviti prava pitanja koja će vam pomoći da donesete ispravnu odluku. Dvije najvažnije stvari koje se treba usredotočiti su:

- Snaga procesiranja (tj. Koliko ćete obrade raditi na rubu?)
- Količina lokalne pohrane podataka (tj. Veličina tvrdog diska - koliko podataka trebate pohraniti?)

Odluke koje donesete vi i vaš tim imati će direktnu povezanost s performansama, funkcionalnošću, troškovima, veličinom uređaja, korisnim vijekom trajanja itd.

Kolika vam je potrebna procesorska snaga?

Da biste odredili koliko snage procesiranja treba vašem uređaju, trebali biste započeti s razumijevanjem svih različitih zadataka koje uređaj mora obaviti.

Stavke koje će utjecati na vašu odluku uključuju:

- Koliko senzora trebate pročitati? (Više senzora će zahtijevati više snage obrade.)
- Trebate li provoditi kontrolu u stvarnom vremenu? (Ovo će definitivno povećati potrebnu moć obrade.)
- Mora li vaša aplikacija vršiti analizu podataka? (Ovo će također povećati potrebnu moć obrade.)
- Imate li dovoljno procesorske snage da podržite buduće nadogradnje / izdanja softvera? (Vaša nova i poboljšana nadogradnja softvera vjerojatno će trebati više snage za obradu.)
- Koja su ograničenja veličine vašeg uređaja? (Na primjer, Fitbit ima samo toliko prostora, ograničavajući veličinu računala i procesorsku snagu.)

Koliko lokalnog prostora za pohranu trebate?

Količina potrebne lokalne pohrane ovisi o pravilima čuvanja podataka. Jednom kada definirate koliko podataka trebate pribaviti, koliko često i koliko ćete slati u Cloud, tada možete izračunati koliko će vam biti potrebno lokalno pohranjivanje kao privremena pohrana za izračun ili da biste služili kao međuspremnik u slučaju gubite vezu s Cloud-om.

Ako se očekuje da vaš proizvod radi izvan mreže, morate odrediti koliko dugo će raditi bez veze, a samim tim i koliko podataka trebate da biste mogli lokalno pohranjivati. Neke aplikacije ne zahtijevaju nikakve prekide u podacima bilo zato što Cloud Analytics neće moći obraditi nedostatke podataka ili zato što imate ugovor s kupcem o kontinuitetu podataka.

4. Komunikacijski modul

Posljednji građevni blok hardvera vašeg uređaja je komunikacijski modul. Ovo je krug koji omogućava komunikaciju s vašom IoT Platformom i sa sistemina trećih strana lokalno ili u Cloudu.

Ovaj modul može uključivati komunikacijske portove kao što su USB, serijski (232/485), CAN ili Modbus. Također može uključivati radio tehnologiju za bežičnu komunikaciju kao što su Wi-Fi, LoRA, ZigBee, itd.

Komunikacijski modul može biti uključen u istom uređaju kao i ostali vaši moduli ili bi to mogao biti zaseban uređaj koji je posebno namijenjen komunikaciji. Ovaj se pristup često naziva „arhitekturom gateway-a“.

Na primjer, ako u sobi imate tri senzora koji trebaju poslati podatke u Cloud, možda bi ti senzori bili povezani na jedan gateway u toj istoj sobi, a gateway objedinjuje te podatke i šalje ih u oblak. Na taj način vam je potreban samo jedan komunikacijski modul, a ne tri.

IoT senzori

Industrije i organizacije već duže vrijeme koriste razne vrste senzora, ali pojava Internet of Things podigao je evoluciju senzora na sasvim drugu razinu.

IoT platforme funkcioniraju i isporučuju različite vrste inteligencije i podataka koristeći različite senzore. Senzori za prikupljanje, slanje i dijeljenje podataka s cijelom mrežom povezanih uređaja. Svi ti prikupljeni podaci omogućuju uređajima da autonomno funkcioniraju, a cijeli ekosustav svakim danom postaje „pametniji“.

Fizički uređaji koji imaju ugrađene senzore I komunikacijske mreže dijele informacije jedan s drugim i poboljšavaju njihovu efikasnost i funkcionalnost.

Uzmite Tesla vozila kao primjer. Svi senzori na automobilu bilježe svoju percepciju okoline, prenoseći podatke u ogromnu bazu podataka. Podaci se zatim obrađuju, a svi važni novi podaci šalju se na sva ostala vozila. Ovo je proces koji traje, kroz koji čitav vozni park Teslina vozila svakim danom postaje pametniji.

To je samo jedan primjer.

Kako što smo već saznali, IoT tehnologija pomaže rastućem broju fizičkih uređaja da postanu pametni, povezani uređaji koji pružaju mogućnosti daleko iznad tradicionalnih fizičkih uređaja.

U ovom procesu senzori izgraju nezamjenjivu ulogu.

Pogledajmo neke od ključnih senzora koji se široko koriste u svijetu IoT-a.

1. Senzori temperature (eng. Temperature sensors)

Po definiciji, "uređaj koji se koristi za mjerenje količine toplinske energije koji omogućava otkrivanje fizičke promjene temperature iz određenog izvora i pretvara podatke za uređaj ili korisnika, poznat je kao temperaturni senzor."

Prije samo nekoliko godina njihova upotreba uglavnom je uključivala klima uređaj, hladnjake i slične uređaje koji se koriste za kontrolu okoliša. Međutim, dolaskom u svijet IoT-a oni su pronašli svoju ulogu u proizvodnim procesima, poljoprivredi i zdravstvenoj industriji.

U procesu proizvodnje, mnogim strojevima je potrebna specifična temperatura okoliša, kao i temperatura uređaja. Ovakvim načinom mjerenja postupak proizvodnje uvijek može ostati optimalan.

S druge strane, u poljoprivredi je temperatura tla presudna za rast usjeva. To pomaže u proizvodnji biljaka, maksimizirajući proizvodnju.

Slijede neke podkategorije temperaturnih senzora:

- **Termoparovi (eng. Thermocouples)**: ovo su naponski uređaji koji označavaju mjerenje temperature s promjenom napona. Kako temperatura raste, izlazni napon termoelementa raste.
- **Detektor temperature otpornika (RTD)**: Otpor uređaja je izravno proporcionalan temperaturi, povećavajte se u pozitivnom smjeru kad temperatura raste, a otpor raste prema gore.
- **Termistori**: To je temperaturni otpornik koji mijenja fizički otpor promjenom temperature.
- **IC (poluvodiči)**: Oni su linearni uređaji gdje se vodljivost poluvodiča linearno povećava i koristi svojstva varijabilnih otpora poluvodičkih materijala. Može osigurati direktno očitavanje temperature u digitalnom obliku, posebno na niskim temperaturama.
- **Infracrveni senzori**: Ovi senzori detektuju temperaturu presretanjem dijela emitirane infracrvene energije predmeta ili tvari i osjetivši njen intenzitet, može se koristiti za mjerenje temperature krutih tvari i tekućina, a nije ih moguće koristiti na plinovima zbog njihove prozirne prirode.

2. Senzori blizine (eng. Proximity sensors)

Senzori blizine pomažu uređaju da otkrije prisutnost ili odsutnost obližnjeg objekta ili svojstava tog objekta i pretvara ga u signal koji korisnik može lako pročitati ili koji se može poslati na drugi uređaj.

Senzori blizine uglavnom se koriste u maloprodaji, jer mogu otkriti kretanje I korelaciju kupca i proizvoda koji bi ih mogli zanimati. Korisnik je odmah obaviješten o popustima i posebnim ponudama proizvoda u blizini.

Drugi veliki i prilično stari slučaj uporabe jesu vozila. Kada vozite unazad ili unaza taj posao obavljaju senzori blizine. Koriste se i za dostupnost parkiranja na mjestima kao što su tržni centri, stadioni ili zračne luke.

Vama na raspolaganju stoje nekoliko podkategorija senzora blizine:

- **Induktivni senzori**: Induktivni blizinski senzori koriste se za beskontaktno otkrivanje kako bi se utvrdila prisutnost metalnih predmeta pomoću elektromagnetskog polja ili snopa elektromagnetskog zračenja. Može raditi pri većim brzinama od mehaničkih sklopki, a također se čini pouzdanijim zbog svoje robusnosti.
- **Kapacitivni senzori**: Kapacitivni senzori blizine mogu otkriti metalne i nemetalne ciljeve. Gotovo svi drugi materijali su različiti od zraka. Može se koristiti za primjećivanje vrlo malih predmeta kroz veliki dio područja. Dakle, obično se koristi u teškim i kompliciranim primjenama.
- **Fotoelektrični senzori**: Fotoelektrični senzor sastoji se od dijelova osjetljivih na svjetlost i koristi snop svjetlosti za otkrivanje prisutnosti ili odsutnosti predmeta. Idealna je alternativa induktivnim senzorima. Koristi se za daljinsko otkrivanje ili za osjet metala ne-metalnih predmeta.
- **Ultrazvučni senzori**: Ultrazvučni senzori također se koriste za otkrivanje prisutnosti ili za mjerenje udaljenosti ciljeva sličnih radaru ili sonaru. To čini pouzdano rješenje za teške i zahtjevne uvjete.

Tip:

Automobili koji imaju parking senzore obično koriste elektromangnetne ili ultrazvučne senzore.

3. Senzor pritiska

Senzor pritiska je uređaj koji osjeti pritisak i pretvara ga u električni signal.

Puno je uređaja koji se oslanjaju na tekući ili drugi oblik pritiska. Ovi senzori omogućuju stvaranje IoT sustava koji nadgledaju sisteme i uređaje pod pritiskom. S bilo kakvim odstupanjem od standardnog raspona pritiska, uređaj obavještava administratora sistema ili korisnika o bilo kakvim problemima koje treba riješiti.

Upotreba ovih senzora nije samo korisna u proizvodnji, I autoindustriji (već dugo novi automobile moraju imati ugrađene senzore pritiska u pneumaticima) već i u održavanju cijelih vodovodnih sisitema i sistema grijanja, jer je lako otkriti bilo kakvo kolebanje ili pad pritiska.

4. Senzori kvalitete vode

Senzori kvalitete vode koriste se za otkrivanje kakvoće vode i jonskog nadzora prvenstveno u sustavima distribucije vode.

Voda se praktički koristi svugdje. Ovi senzori igraju važnu ulogu jer prate kvalitetu vode u različite svrhe. Koriste se u raznim industrijama.

5. Hemijski senzori

Hemijski senzori primjenjuju se u brojnim industrijama. Njihov je cilj naznačiti promjene tekućine ili otkriti kemijske promjene u zraku. Oni igraju važnu ulogu u većim gradovima, gdje je potrebno pratiti promjene i zaštititi stanovništvo.

Slučajevi glavne upotrebe hemijskih senzora mogu se naći u nadzoru industrijskog okoliša i kontroli procesa, namjerno ili slučajno puštenom detekciji štetnih kemikalija, detekciji eksploziva i radioaktivnosti, recikliranju u svemirskoj stanici, farmaceutskoj industriji i laboratoriju itd.

6. Senzor plina

Senzori plina slični su hemijskim, ali posebno se koriste za nadziranje promjena kvalitete zraka i otkrivanje prisutnosti različitih plinova. Kao i hemijski senzori, oni se koriste u brojnim industrijama kao što su proizvodnja, poljoprivreda i zdravstvo, a koriste se za praćenje kvaliteta zraka, otkrivanje otrovnih ili zapaljivih plinova, praćenje opasnih plinova u rudnicima ugljena, naftna i plinska industrija, kemijska laboratorijska istraživanja, proizvodnja - boje , plastika, guma, farmacija i petrokemija itd.

Evo nekoliko uobičajenih senzora za plin:

- Senzor ugljičnog dioksida
- Analiza daha (eng. Breathalyzer)
- Detektor ugljičnog monoksida
- Senzor vodika
- Senzor zagađenja zraka
- Senzor dušikovog oksida
- Senzor kisika
- Ozonski monitor
- Elektrokemijski senzor plina
- Detektor plina.

7. Senzor dima

Senzor dima uređaj je koji osjeća dim (čestice i plinovi u zraku) i to na razini.

Već su dulje vrijeme u upotrebi. No, s razvojem IoT-a oni su sada još efikasniji jer su priključeni na sistem koji odmah obavještava korisnika o bilo kojem problemu koji se dogodi u različitim industrijama.

Senzori dima široko se koriste u proizvodnoj industriji, klimatizacijskim uređajima, zgradama i smještajnim objektima za otkrivanje pojave požara i plina. Ovo služi za zaštitu ljudi koji rade u opasnim okruženjima jer je cijeli sustav mnogo učinkovitiji u odnosu na starije.

8. IR senzori

Infracrveni senzor je senzor koji se koristi za osjetiti određene karakteristike njegove okoline bilo da emitira ili detektira infracrveno zračenje. Također je u mogućnosti mjeriti toplinu koju emitiraju objekti.

Sada se koriste u raznim IoT projektima i širokom nizu redovnih pametnih uređaja, kao što su pametni satovi i pametni telefoni.

Druga uobičajena upotreba uključuje kućanske uređaje i daljinski upravljač, analizu daha, infracrveni vid (tj. Vizualizirajte propuštanje topline u elektronici, nadgledate protok krvi, povjesničare umjetnosti da vide ispod slojeva boje), nosivu elektroniku, optičku komunikaciju, mjerenje temperature na bazi beskontaktnih, automobilsko otkrivanje slijepih kuta.

Njihova upotreba tu ne završava, oni su i sjajan alat za osiguranje visoke razine sigurnosti u vašem domu. Također, njihova primjena uključuje provjere okoliša jer mogu otkriti razne kemikalije i toplinske curenje. Oni će igrati važnu ulogu u industriji pametnih kuća jer imaju širok raspon primjena.

9. Senzori razine

Senzor koji se koristi za određivanje razine ili količine tekućine, tekućina ili drugih tvari koje teku u otvorenom ili zatvorenom sustavu naziva se Senzor razine.

Kao i IR senzori, senzori razine prisutni su u širokom rasponu industrije. Oni su prije svega poznati po mjerenju razine goriva, ali se također koriste u kompanijama koje rade s tekućim materijalima. Na primjer, industrija recikliranja, kao i industrija sokova i alkohola oslanjaju se na ove senzore za mjerenje broja likvidnih sredstava u njihovom vlasništvu.

Najbolji slučajevi korištenja senzora nivoa su, ispitivanje razine goriva i razine tekućine u otvorenim ili zatvorenim spremnicima, nadzor razine mora i upozorenje za cunami, rezervoari vode, medicinska oprema, kompresori, hidraulični spremnici, alatni strojevi, pića i farmaceutska obrada, visoka ili niska razina otkrivanje itd.

To pomaže boljem pojednostavljivanju poslovanja jer senzori prikupljaju sve važne podatke u svakom trenutku. Upotrebom ovih senzora svaki upravitelj proizvoda može precizno vidjeti koliko je tekućine spremno za distribuciju i treba li pojačati proizvodnju.

10. Senzori slike

Senzori slike su instrumenti koji se koriste za pretvaranje optičkih slika u elektroničke signale za elektroničko prikazivanje ili pohranu datoteka.

Najveću uporabu senzora slike nalazimo u digitalnim fotoaparatima i modulima, medicinskoj snimci i opremi za noćno gledanje, uređajima za termičko snimanje, radaru, sonaru, medijskoj kući, biometrijskim i IRIS uređajima.

Dvije glavne vrste senzora koriste se u:

- CCD (uređaj povezan s punjenjem) i
- CMOS (komplementarni poluvodički metal-oksid) slike.

Iako svaka vrsta senzora koristi drugačiju tehnologiju za snimanje slika, i CCD i CMOS uređaji koriste poluvodiče metal-oksid, koji imaju isti stupanj osjetljivosti na svjetlost i nemaju svojstvenu razliku u kvaliteti

Prosječni potrošač pomislio bi da je to obična kamera, ali iako to nije daleko od istine, senzori slike povezani su sa širokim rasponom različitih uređaja, što njihovu funkcionalnost čini znatno boljom.

Jedna od najpoznatijih primjena uključuje automobilsku industriju, u kojoj slike imaju vrlo važnu ulogu. Pomoću ovih senzora system može prepoznati znakove, prepreke i mnoge druge stvari koje vozač obično primijeti na cesti. Oni imaju vrlo važnu ulogu u IoT industriji, jer izravno utječu na napredak automobila bez vozača.

Također se provode u poboljšanim sigurnosnim sustavima, gdje slike pomažu u snimanju detalja o počinitelju.

U maloprodajnoj industriji ovi senzori služe za prikupljanje podataka o kupcima, pomažući kompanijama da steknu bolji uvid u to tko zapravo posjećuje njihovu trgovinu, rasa, spol, dob samo su neki od korisnih parametara koje vlasnici maloprodaje dobivaju pomoću ovih IoT senzora.

11. Senzori za otkrivanje pokreta

Detektor pokreta je elektronički uređaj koji se koristi za otkrivanje fizičkog kretanja u određenom području i pretvara kretanje u električni signal; gibanje bilo kojeg predmeta ili kretanja ljudi

Otkrivanje pokreta igra važnu ulogu u sigurnosnoj industriji. Tvrtke koriste ove senzore na područjima u kojima ne smije stalno otkrivati kretanje, i lako je primijetiti da je nečija prisutnost sa instaliranim tim senzorima.

Primarno se koriste za sisteme za otkrivanje provale, automatizaciju vrata, zaštitne zavjese, pametnu kameru (tj. Snimanje zasnovano na pokretu / video snimanje), naplatu cestarine, automatsko parkiranje, automatizirane sudopere, sušilice za ruke, sustave upravljanja energijom (tj. Automatizirani Rasvjeta, izmjenična struja, ventilator, kontrola uređaja) itd.

S druge strane, ti senzori također mogu dešifrirati različite vrste pokreta, što ih čini korisnim u nekim industrijama u kojima kupac može komunicirati sa sistemom mahanjem ruku ili izvršavanjem slične akcije. Na primjer, netko može mahnuti senzoru u maloprodaji kako bi zatražio pomoć u donošenju ispravne odluke o kupnji.

Iako je njihova napredna upotreba povezana sa sigurnosnom industrijom, kako tehnologija napreduje, broj mogućih primjena ovih senzora tek će rasti.

Slijede ključni tipovi senzora pokreta koji se široko koriste:

- **Pasivno infracrveno (PIR)**: Otkriva tjelesnu toplinu (infracrvena energija) i najčešće korišteni senzor pokreta u kućnim sigurnosnim sustavima.
- **Ultrazvučni**: odašilje impulse ultrazvučnih valova i mjeri odraz od pokretnog predmeta praćenjem brzine zvučnih valova.
- **Mikrotalasna**: emitira radio valove impulse i mjeri odraz od pokretnog predmeta. Pokrivaju veće područje od infracrvenih i ultrazvučnih senzora, ali podložni su električnim smetnjama i skuplji su.

12. Senzori za akcelerometar

Akcelerometar je pretvarač koji se koristi za mjerenje fizičkog ili mjerljivog ubrzanja koje doživljava objekt uslijed inercijalnih sila i pretvara mehaničko gibanje u električni izlaz. Definira se kao stopa promjene brzine s obzirom na vrijeme

Ti su senzori prisutni na milijunima uređaja, poput pametnih telefona. Njihove uporabe uključuju otkrivanje vibracija, naginjanje i ubrzanje u cjelini. Ovo je izvrsno za nadgledanje voznog parka ili korištenje pametnog pedometra.

U nekim se slučajevima koristi kao oblik zaštite od krađe, jer senzor može poslati upozorenje kroz sustav ako se pomakne objekt koji bi trebao ostati nepomičan.

Oni se široko koriste u mobilnim i medijskim uređajima, mjerenju vibracija, automobilskoj kontroli i detekciji, otkrivanju slobodnog pada, zrakoplovstvu i zrakoplovnoj industriji, detekciji kretanja, nadzoru ponašanja sportske akademije / sportaša, potrošačkoj elektronici, industrijskim i gradilištima itd.

Postoje različite vrste akcelerometara, a nekoliko njih uglavnom se koristi u IoT projektima:

- **Akcelerometri Hall-Effect**: Hall-efekt mjerači ubrzanja koriste Hall princip za mjerenje ubrzanja, oni mjere promjene napona uzrokovane promjenama magnetskog polja oko njih.

- **Kapacitivni akcelerometri**: Kapacitivni akcelerometri koji osjećaju ovisne vrijednosti izlaznog napona o udaljenosti između dviju ravnina. Kapacitivni akcelerometri također su manje skloni buci i promjenama temperature.
- **Piezoelektrični akcelerometri**: Piezoelektrični senzorski princip djeluje na piezoelektrični učinak. Akcelerometri na bazi piezo filma najbolje se koriste za mjerenje vibracija, udara i pritiska.

Svaka tehnologija senzora akcelerometra ima svoje prednosti i kompromise. Prije odabira važno je razumjeti osnovne razlike različitih vrsta i zahtjeve ispitivanja.

13. Žiroskopski senzori

Senzor ili uređaj koji se koristi za mjerenje ugaone brzine poznat je kao Gyro senzori. Ugaona brzina jednostavno se definira kao mjerenje brzine vrtnje oko neke osi. To je uređaj koji se prvenstveno koristi za navigaciju i mjerenje ugaone i rotacijske brzine u smjeru 3 osi. Najvažnija aplikacija je nadgledanje orijentacije objekta.

Njihove se glavne primjene nalaze u automobilskim navigacijskim sustavima, kontrolerima igara, mobilnim uređajima i kamerama, elektroničkoj potrošnji, kontroli robotike, upravljanju bespilotnim i RC upravljačkim helikopterima ili UAV, upravljanju vozilima / ADAS i mnogim drugim.

Postoji nekoliko različitih vrsta žiro senzora koje se biraju prema radnom mehanizmu, vrsti izlaza, snazi, rasponu osjetljivosti i uvjetima okoline.

- Rotacijski (klasični) žiroskopi
- Žiroskop za vibrirajuću strukturu
- Optički žiroskopi
- MEMS (mikro-elektro-mehanički sustavi) Žiroskopi

Ovi su senzori uvijek kombinirani s akcelerometrima. Upotreba ova dva senzora jednostavno daje više povratnih informacija sustavu. S instaliranim žiroskopskim senzorima, mnogi uređaji mogu pomoći sportašima u poboljšanju učinkovitosti njihovih pokreta, jer tijekom sportskih aktivnosti dobivaju pristup sportašima.

Ovo je samo jedan primjer njegove primjene, međutim, kako je uloga ovog senzora da otkriva rotaciju ili uvijanje, njegova je primjena presudna za automatizaciju nekih proizvodnih procesa.

14. Senzori vlažnosti

Vlažnost je definirana kao količina vodene pare u atmosferi zraka ili drugih plinova. Najčešće korišteni izrazi su "Relativna vlaga (RH)"

Ovi senzori obično prate uporabu senzora temperature, jer mnogi proizvodni procesi zahtijevaju savršene radne uvjete. Mjerenjem vlažnosti možete osigurati da cijeli proces teče bez problema, a kad dođe do nagle promjene, možete poduzeti mjere odmah, jer senzori detektiraju promjenu gotovo trenutno.

Njihove primjene i upotreba mogu se naći u industrijskoj i stambenoj domeni za upravljanje sustavima grijanja, ventilacije i klimatizacije. Oni se mogu naći u automobilskoj industriji, muzejima, industrijskim prostorima i staklenicima, meteorološkim stanicama, industriji boja i premaza, bolnicama i farmaceutskoj industriji radi zaštite lijekova

15. Optički senzori

Senzor koji mjeri fizičku količinu svjetlosnih zraka i pretvara je u električni signal koji korisnik može lako čitati ili se elektronički instrument / uređaj naziva optički senzor.

Stručnjaci IoT-a vole optičke senzore jer su praktični za istovremeno mjerenje različitih stvari. Tehnologija koja stoji iza ovog senzora omogućava mu praćenje elektromagnetske energije, što uključuje električnu energiju, svjetlost i tako dalje.

Zbog ove su činjenice ovi senzori našli upotrebu u zdravstvu, nadzoru okoliša, energetici, zrakoplovstvu i mnogim drugim industrijama. Svojom prisutnošću naftne kompanije, farmaceutske kompanije i rudarske kompanije nalaze se u mnogo boljem položaju za praćenje promjena u okolišu, čuvajući svoje zaposlenike.

Njihova se glavna upotreba može naći u detekciji ambijentalne svjetlosti, digitalnim optičkim prekidačima, komunikaciji s optičkim vlaknima, zbog električne izolacije koja je najprikladnija za primjenu nafte i plina, civilna i transportna polja, mrežni sustavi velike brzine, upravljanje vratima dizala, brojači dijelova montažnih vodova i sigurnosni sustavi.

Slijede ključne tipovi optičkih senzora:

- **Fotodetector**: Upotrebljava fotodetektor za upotrebu polutodiktorskih materijala osjetljivih na svjetlost kao što su fotoćelije, fotodiodi ili fototransistori.
- **Optička vlakna**: Vlakna optika ne nosi struju, tako da je imuno na električnu i elektromagnetsku interferenciju, pa čak ni u oštećenom stanju, ne postoji opasnost od iskrenja ili udara.
- **Pirometar**: Procjenjuje temperaturu objekta tako što osjeti boju svjetla koju zrače objekti prema njihovoj temperaturi i proizvode iste boje na istoj temperaturi.
- **Blizinski i infracrveni**: Blizinski senzor koristi svjetlost kako bi osjetio objekte u blizini, a infracrveni koristi se tamo gdje bi vidljiva svjetlost bila jako slaba.

Jasno je da je IoT postao nevjerojatno popularan, a trenutni trendovi pokazuju da je to budućnost. Jednostavno pomaže u automatizaciji različitih procesa, čineći ove sustave vrlo korisnim za redovite potrošače i tvrtke.

Tek treba vidjeti puni potencijal koji ova tehnologija nosi s obzirom da je cijela platforma sve pametnija zbog fuzije svih gore spomenutih senzora. Kada uzmete u obzir činjenicu da su svi mjereni podaci prikupljeni i mogu se analizirati, očito je da će IoT u budućnosti postati još pametniji.

2. Odabir najboljeg hardvera za IoT projekat

Karakteristike IoT uređaja; Hardver za razvoj protipa IoT projekta; Hardverski zahtjevi za implementaciju komercijalnog IoT projekta

Karakteristike IoT uređaja

U prehodnoj sekciji ste mogli saznati zašto su povezani uređaji centralni dio za IoT. Uređaji prikupljaju podatke i prate parametre.
Nalaze se na svemu, od industrijske opreme, zgrada i automobila, do životinja, pošiljaka tereta, cjevovoda i ljudi.
Hardverske i softverske komponente dizajnirane su za IoT aplikacije putem standardnog protokola dizajna koji uključuje: razvoj specifikacija, idejni dizajn, prototip, testiranje i na kraju razvoj hardvera i softvera koji su integrirani u mrežu.
Neke platforme, kao što su Arduino i Raspberry Pi, mogu ubrzati dizajn i omogućiti brzo prototipiranje bez uključivanja prilagođavanja, ubrzavajući tako vrijeme potrebno za implementaciju IoT konfiguracije.
Dizajn će zahtijevati identifikaciju zahtjeva za performansama, potrebnog hardvera i softvera da bi se postigli takvi zahtjevi, a zatim specifikacije za komponente - ili komercijalnih komponenti koje možete nabaviti na tržištu (Commerciality off-the-shelf COTS) ili komponenti koje su prilagođene vašem dizajnu - s dužnim razmatranjem operativnog okruženja i aplikacije koja treba biti koristi se u njemu.
U kontekstu IoT-a, uređaj se odnosi na sve što sadrži informacije i prenosi ih.
Na primjer, senzor pritiska u cjevovodu, senzor temperature unutar rashladnog vagona ili sitni čips koji se nalazi oko vrata krava - svi su uređaji.
Uređaji mogu biti samostalni ili raditi u sinkronizaciji s drugim uređajima.

U ovoj sekciji imaćete prilike da se upoznate sa nekim off-the-shelf hardverskim opcijama i faktorima koje možete uzeti u obzir pri odabiru za razvoj vašeg sljedećeg IoT projekta.

Ključne karakteristike IoT uređaja

Kako se IoT okruženjek razvija, uvode se novi uređaji i platforme. Postoje ključne karakteristike koje su zajedničke IoT uređajima koji daju osnovu za usporedbu pri odabiru hardvera i softvera za konfiguriranje nove IoT mreže ili za razvoj i proširenje postojeće.

Uređaji IoT mogu se okarakterizirati po mogućnostima za:

- Prikupljanje i kontrola podataka
- Obrada i pohrana podataka
- Povezivanje
- Upravljanje napajanjem

Kao što možete primjetiti mogućnosti IoT hardvera kategorisane na sličan način kao što smo predhodnoj sekciji opisali četri gradivna bloka IoT hardvera.

Pogledajmo koje su to njihove specifične mogućnosti.

Prikupljanje i kontrola podataka

Prikupljanje podataka (eng. Data acquisition - DAQ) prikuplja analogne podatke u određenom vremenskom intervalu (brzina uzorkovanja podataka) i šalje ih kao digitalni signal na udaljeni izlazni uređaj za digitalno očitavanje.

DAQ može uključivati kondicioniranje signala (za manipuliranje i skaliranje očitavanja neobrađenih očitavanja) i analogno-digitalne pretvarače za pretvaranje očitavanja analognih senzora u digitalne vrijednosti kako bi se mogli obraditi i analizirati.

Senzori su komponente koje mjere fizičke varijable i pretvaraju ih u električne signale (napone). Senzori su dostupni komercijalno, a određeni su za mjerenje niza varijabli koje uključuju: temperaturu, vlažnost, tlak, dim, plin, svjetlost, zvuk, vibracije, protok zraka, protok vode, brzinu, ubrzanje , blizina, GPS položaj, nadmorska visina i mnoštvo drugih parametara.

Senzori se razlikuju po svojoj funkcionalnosti i mogu se koristiti za mjerenje širokog spektra stanja. Na primjer, proprioceptivni senzori prate unutarnje stanje uređaja. Senzori poput tipki, kliznih kontrola ili dodirnih ekrana mogu se koristiti za direktno komuniciranje s uređajem (interfejs čovjeka i stroja).

Već ste se mogli upoznati da svaka vrsta senzora ima mnogo mogućnosti. Proizvođači i njihove specifikacije proizvoda senzora se razlikuju. Tačnost, preciznost i potrebni radni uslovi senzora mogu se razlikovati od kataloga do kataloga i od proizvođača do proizvođača.

Senzori se mogu koristiti unutar motora, pod vodom, ugrađenih u objekte ili uređaje. Okruženje zahtijeva različite karakteristike senzora i osmišljeno je za različite namjene.

Važna karakteristika komponenata senzora je rezolucija.

Rezolucija senzora predstavlja najmanju količinu promjena koje senzor može pouzdano očitati i povezana je s veličinom numeričke vrijednosti koja se koristi za predstavljanje

nepročišćenih očitavanja senzora. Na primjer, analogni temperaturni senzor s rezolucijom od 10 bita predstavlja očitanje temperature koristeći numeričku vrijednost između 0 i 1023. Bitovi su binarni, tako da 10 bita daje dvije na ukupno 10 ili 1024 mogućih vrijednosti. Međutim, u praksi na senzore utječe električni šum koji smanjuje stvarnu rezoluciju.

Dok senzori pretvaraju fizičku varijablu poput temperature u električni signal, izlazni uređaji su obrnuti: električni signal pretvaraju u fizički ishod.

Izlazni uređaji uključuju LED, zvučnike i zaslone.

To može zahtijevati pogone poput motora, releja i solenoida koji nešto fizički aktiviraju.

Aktuatori su uobičajeni u industrijskim IoT aplikacijama.

Na primjer, pneumatski linearni aktuatori su široko prihvaćeni u proizvodnji za pomicanje i prianjanje proizvoda tijekom postupka montaže. Pokretač na osovini automobila može aktivirati kočenje kad se utvrdi nepovoljno kretanje. Visoka temperatura u rashladnom spremniku s proizvodima iznutra može aktivirati alarm kada temperatura poraste do određene neprihvatljive razine.

Obrada i pohrana podataka

IoT uređaji zahtijevaju specifične mogućnosti obrade i pohrane podataka. To pomaže postići agregaciju, prijenos i analizu podataka. Neki IoT uređaji mogu izravno obrađivati podatke, dok drugi prenose te podatke na druge uređaje, pristupne uređaje ili aplikacije u Cloud-u radi daljnje agregacije i analiza.

Analiza na ruba (eng. Edge analytics) provodi analizu podataka na rubovima mreže, a ne na centraliziranom mjestu. Podaci se mogu analizirati u stvarnom vremenu na samim uređajima ili se mogu analizirati na obližnjem ulaznom uređaju (poput usmjerivača) povezanom s IoT uređajima, umjesto prijenosa velike količine podataka na Cloud servis ili podatkovni centar za daljnje analiza. Obrada podataka na rubu agregira i filtrira podatke dok su prikupljeni, a samo su najvidljiviji podaci se salju na server. Analiza ruba smanjuje zahtjeve za obradu i skladištenje na server (ili Cloud-u), što smanjuje opterećenje mreže.

Snaga obrade i pohrana koju koristi IoT aplikacija zavisi o obradi koju zahtijevaju usluge ili aplikacije koje konzumiraju podatke. Dostupne specifikacije memorije i procesora, brzina takta i broj jezgara, a sve kasnije određuje brzina procesiranja uređaja. Kapacitet memorije koja ne zahtjeva napajanje (eng. Non-volatile flash), koji se koristi za obnavljanje podataka dok se ne prenose na server, određuje koliko podataka može biti pohranjeno na uređaju. Uređaji koji obavljaju rubnu analitiku zahtijevaju znatno više

mogućnosti obrade od uređaja koji izvode samo osnovne obrade podataka poput provjere valjanosti, normalizacije, skaliranja ili pretvaranja očitanja.

Povezivanje

Mrežna povezanost je definirajuća karakteristika bilo kojeg IoT uređaja.

Uređaji komuniciraju s drugim uređajima lokalno. Zatim objavljuju podatke putem usluga utemeljenih na platform ili Cloud servisu.

Neki uređaji komuniciraju bežično, koristeći 802.11 (Wi-Fi), Bluetooth, RFID, mobilne mreže ili širokopojasnu mrežu široke mreže (LPWAN) poput LoRa, SigFox ili NB-IoT.

Žžičena komunikacija odgovara stacionarnim uređajima.

Takvi se uređaji mogu instalirati, na primjer, u pametne zgrade, automatizaciju domova i industrijske kontrole, te povezati s Ethernetom ili ih možda dodatno opremiti Ethernetom preko snage. Serijska komunikacija je oblik ožičene povezanosti između uređaja pomoću standardnih protokola poput univerzalnog asinhronog odašiljača (UART) ili protokola Controller Area Network (CAN), koji ima svoje podrijetlo u automobilskoj industriji.

Upravljanje napajanjem

Upravljanje napajanjem je kritični faktor za prijenosne i nosive IoT uređaje koji se oslanjaju na bežični izvor napajanja, poput baterija ili fotonaponskih ćelija (solarno). Zavise o obrascima upotrebe i potrebama napajanja priključenih senzora, aktuatora ili integriranog kruga (IC), uređaj se može povremeno prebacivati u stanje mirovanja ili u način slabe potrošnje radi uštede energije.

Na primjer, jedno-ploćnom računaru kao što je Raspberry Pi 4 potrebno je oko 700 - 1000 mA struje da radi pod uobičajenim načinom rada. Ako ste neprestano prenosili podatke putem wifi mreže ili ako je uređaj pod velikim opterećenjem vršio veliku obradu podataka, potrošnja energije bi bila velika, ali onda bi se smanjila kada uređaj ne radi. Ako spojite modul kamere, potrebna amperaža se povećava za oko 250mA kad se kamera koristi. Takođe, senzorima je normalno potrebna snaga za rad; GPIO pinovi na Raspberry Pi napajanju 3.3V ili 5V, do ukupno 50mA struje u svim pinovima. Potrošnja energije uređaja povećava se s povećanjem broja komponenti koje su pričvršćene na pinove kompjutera.

Hardver za razvoj prototipa IoT projekta

Razvoj IoT aplikacija je pristupačniji s rastućom dostupnošću jeftinih, komercijalno dostupnih hardverskih razvojnih ploča, platformi i seta za izradu prototipa.

Popularnost IoT dovela je do toga da nam na raspolaganju stoji širok spektar modularno dizajniranog hardvera koji nam pruža veliku fleksibilnost u razvoju IoT projekta.

S većim izborom komponenti, dizajneri mogu zamijeniti nove senzore s različitim specifikacijama. Alternativno, možete samostalno nadograditi mreže, obradu podataka ili module za pohranu uređaja za evoluirajuće potrebe. Mnogi komercijalni hardverski uređaji, uključujući mikrokontrolere i jedno-pločna računala, dizajnirani su oko integriranih krugova "Sistem na čipu (eng. System-on-a-Chip SoC).

SoC obezbjeđuje mogućnost da korištenjem samo jednog čipa obezbjedite paket koji može vršiti funkcije obrada podataka, skladištenja i umrežavanja.

Ova konfiguracija znači da žrtvujete određenu fleksibilnost radi praktičnosti, ali, srećom, na raspolaganju je ogroman broj robnih uređaja s nizom konfiguracija. Na primjer, u narednoj tabeli nalaze se tehničke specifikacije za izbor mikrokontrolera koji se mogu koristiti za prototipiranje IoT projekata i pruža usporedbu tri popularna računara sa jednom pločom (Single-Board-Computers - SBC).

Ploče za razvoj mikrokontrolera

Mikrokontroler je SoC koji pruža mogućnosti obrade i pohrane podataka. Mikrokontroleri sadrže jezgru procesora (ili jezgre), memoriju (RAM) i izbrisljivu programibilnu memoriju za čitanje (EPROM) za pohranu prilagođenih programa koji se izvode na mikrokontroleru. Razvojne ploče mikrokontrolera su štampane ploće (eng. Printed Circuit Board PCB) s dodatnim sklopovima koji podržavaju mikrokontroler kako bi bilo pogodnije za prototiranje i programiranje čipa.

Senzori i aktuatori povezuju se s mikrokontrolerom putem digitalnih ili analognih ulaza / izlaza opće namjene (eng. General Pirpose Input/output - GPIO) ili preko hardverske sabiirnice. Standardni komunikacijski protokoli poput I2C (eng. Inter-integrated Circuit) i SPI (eng. Serial Peripheral Interface) koriste se za komunikaciju unutar uređaja s komponentama koje su povezane sa sabirnicom. Usvajanje standarda olakšava dodavanje ili zamjenu dijelova koji su povezani sa sabirnicom.

Jedna od najzastupljenijih ploča za razvoj mikrokontrolera je Arduino.

Arduino je platforma uređaja otvorenog koda, s aktivnom zajednicom koja stvara kompatibilne razvojne ploče i alate. Mogućnosti uređaja razlikuju se između službenih

Arduino modela (https://www.arduino.cc/en/Products/Compare)), kao i između desetaka kompatibilnih ploča treće strane. Svi uređaji nalaze se u Arduino kompatibilnim mikrokontrolerima, uključujući sveprisutni Arduino Uno, Particle's Electron, koji uključuje integrirani stanični modem, i Espressif Systems '(ESP8266-01, mikrokontroler niske potrošnje, s ugrađenim wifi-jem.

Kao i Arduino, ESP8266 ima aktivnu zajednicu korisnika. Značajni razvojne table koji se temelje na ESP8266 uključuju NodeMCU, WeMos D1 i AdaFruit's Feather Huzzah.

Nekoliko alternativnih opcija firmware-a za ploče koje se temelje na ESP8266 razvile su zajednica otvorenog koda i proizvođač, omogućujući IoT programerima da programiraju za te ploče pomoću Lua, Python-a i JavaScript-a, te da podržavaju over-the-air (OTA) ažuriranja.

Tabela: Tehničke specifikacije za Arduino Uno, Particle Electron I Espressif Systems

Karakteristike	Svojstva	Arduino Uno	Particle Electron	Espressif Systems ESP8266-01
Prikupljanje i kontrola podataka				
	GPIO pins	6 Analog in 14 Digital – 6 PWM	12 Analog in 2 Analog out 30 Digital – 13 PWM	2 Digital 1 Analog
	Logic level voltage	5V	3.3V	3.3V
Procesiranje I skladištenje podataka				
	Processor	ATMega328P	32-bit STM32F205 ARM Cortex M3	32-bit Tensilica L106
	Processor speed	16 KHz	120 MHz	80 MHz
	Memory	32 kB flash, 1 kB EEPROM	1 Mb flash, 128 kB RAM	1 Mb
Povezivanje				
	Network Interfaces	None by default. Can be added with shields.	Integrated cellular modem (2G / 3G)	Integrated wifi
Napajanje				
	Recommended Power Supply	9-12V DC 0.5 – 2A barrel, or 5V 500mA USB, or 9 – 12V on VIN pin	5V micro USB or 3.9V-12VDC on VIN pin	Regulated 3.3V 300mA supply on VCC pin
Ostalo				
	Dimensions	2.7 in X 2.1 in	2.05 in x 0.8 in	1.4 in x 1 in
	Typical cost	$20	$39 – $59	$10

Standardni pristup razvoju softvera za pokretanje na mikrokontrolerima kompatibilnim sa Arduino je upotreba C ili C ++ i Arduino IDE, međutim postoje i jezične veze i alati za vizualno programiranje razvijeni u zajednici.

Arduino-kompatibilne ploče koje imaju zajedničke rasporede pinova moguće je proširiti korištenjem opcionalnih zaštitnih oklopa, na primjer, dodavanju Ethernet porta ili Bluetooth Arduino Uno-u.

Arduino je najčešće prihvaćeno okruženje za razvoj mikrokontrolera za hobiste, ali drugi poput Tessela (https://tessel.io/) i Particle.io (http://particle.io) izvorno podržavaju JavaScript, dok je Python podržan za ploče poput MicroPythonova PyBoard (http://micropython.org) i WeIO (http://we-io.net/hardware/).

Odabirom mikrokontrolera koji podržava Arduino olakšava se prijenos programa koji su razvijeni korištenjem Arduino knjižnica više platformi i Arduino IDE za pokretanje na drugim Arduino kompatibilnim uređajima.

Primjerice, Arduino Uno koristi 5V logiku na digitalnim I / O pinovima (gdje je 0 volti jednako NISKO ili isključeno, a 5 volti jednako VISOKO ili UKLJUČENO), ali ESP8266 i ploče čestica koriste 3.3V logiku (VISOKI je 3.3V).

To može utjecati na izbor senzora ili komponenate aktuatora, jer neke komponente rade samo s jednim ili drugim. Zamijenom senzora koji su dizajnirani za logiku od 5V do 3.3V mogu rezultirati nepredvidivim rezultatima i da se eventualno oštete pinovi koji su netolerantni na veće napone, pa će vam trebati dodati pretvarač razine logike da bi ovo radio. Kad se prebacite na implementaciju hardverskih karakteristika niske razine poput omogućavanja načina dubokog mirovanja ili čitanja s povezanih senzora pomoću posebnih protokola, vjerojatno ćete se morati pouzdati u biblioteke uređaja ili komponente koje će vaš kôd učiniti manje prenosivim.

Računala s jednim pločama

Računala s jednim pločom (SBC) korak su više od mikrokontrolera.

Omogućuju vam priključivanje perifernih uređaja poput tastature, miševa i ekrana, ali i nude više memorije i snage obrade (na primjer, 32-bitni ARM mikroprocesor od 1,2 GHz u usporedbi s 8-bitnim 16KHz mikrokontrolerom).

Naredna tabela navodi tehničke specifikacije za tri SBC-a:

- Raspberry Pi 4,
- BeagleBone Black (http://beagleboard.org/black), i

- DragonBoard 410c (https: //developer.qualcomm com / hardver / dragonboard-410C).

Razlika između mikrokontrolera i računala s jednim pločama donekle je proizvoljna.

Neki uređaji, poput Onion Omega 2 (https://docs.onion.io/omega2-docs/omega2.html#omega2), padaju negdje između, s gotovo isto toliko ugrađene memorije i mogućnosti obrade kao niska - kraj SBC.

Postoji i određeni broj hibridnih uređaja, poput UDOO Quad-a koji integrira ARM-ov Linux sistem s Arduino-kompatibilnim mikrokontrolerom.

Tabela: Tehničke specifikacije za Raspberry Pi 4, BeagleBone Black i DragonBoard SBC

Karakteristike	**Svojstva**	**Raspberry Pi 4**	**BeagleBone Black**	**Qualcomm DragonBoard 410c**
Prikupljanje i kontrola podataka				
	GPIO pins	40 I/O pins, including 29 Digital	65 Digital – 8 PWM 7 Analog in	12 Digital
	Logic level voltage	3.3V	5V	1.8V
Procesiranje I skladištenje podataka				
	Processor	ARM Cortex A72	AM335X ARM Cortex A8	ARM Cortex A53
	Processor speed	1.5GHz	1 GHz	1.2 GHz
	Memory	1-4 Gb	512 Mb RAM, 4 Gb Flash	1Gb, 8Gb Flash
Povezivanje				
	Network Interfaces	Wifi, Ethernet, Bluetooth	Ethernet, USB ports allow xternal wifi / Bluetooth adaptors	Wifi, Bluetooth, GPS
Napajanje				
	Recommended Power Supply	5V 3A USB Type C	5V 1.2A – 2A barrel	6.5 – 18V 2A barrel
Ostalo				
	Dimensions	3.5 x 2.3 in	3.4 x 2.1 in	3.3 in x 2.1 in
	Typical cost	$35	$55	$75

Kao i kod mikrokontrolera, mogućnosti SBC uređaja mogu se proširiti dodavanjem sklopljivih ekspanzijskih ploča poznatih kao *hats* na Raspberry Pi i *capes* na BeagleBone Black, te dodavanjem vanjskih modula, poput kontrolera motora ili analogno-digitalnih pretvarača, koji mogu ublažiti ograničenja ovih uređaja pomoću dodavanja ugradbenih komponenti.

Mnogi SBC uređaji slični su mini-računaru kojeg pokreće ugrađeni operativni sistem, obično pojednostavljenu distribuciju Linuxa. Kao rezultat toga, na raspolaganju je mnogo više razvojnih alata i izbora jezika za razvoj ugrađenih aplikacija koje na tim uređajima rade s priloženim senzorima i aktuatorima nego na mikrokontrolernim pločama. Međutim, SBC-ovi su složeniji za postavljanje, veći i gladniji snage te su skloniji problemima poput oštećenja SD kartice ili flash memorije gdje se pohranjuju aplikacije.

Izbor između razvojnih ploča mikrokontrolera i računala s jednim pločama

Iako su razvojne ploče mikrokontrolera bez ikakvih računara i jednobordnih računala možda samo dio IoT rješenja, oni su idealni za pokretanje novog razvoja.

Jedan od načina za početak je razmotriti ključne karakteristike uređaja IoT s obzirom na zahtjeve vašeg IoT projekta, a zatim proći kroz sljedeće dizajnerske odluke:

- Odredite vrstu i broj perifernih senzora i izlaznih komponenti koje su vam potrebne i, ako je potrebno, bilo koje dizajnerske sklopove za te komponente
- Odaberite mikrokontroler ili uređaj s jednom pločom za koordinaciju očitanja s perifernih komponenata i njihovo upravljanje
- Odlučite se za protokole za prijenos podataka koje trebate koristiti za komunikaciju unutar uređaja (na primjer, korištenje I2C za komunikaciju između mikrokontrolera i bilo kojeg priključenog senzora)
- Odaberite mrežni hardver i protokole koje trebate koristiti za komunikaciju s oblačnim uslugama i aplikacijama

Na primjer, za postavljanje sustava kućne automatizacije, možete odabrati Raspberry Pi Zero W. To je mali i vrlo jeftin SBC uređaj s dovoljnom procesorskom snagom i memorijom (1GHz ARM6 procesor i 512 MB RAM-a) za obavljanje obrade podataka i analitiku na uređaju. Podržava microSD karticu proširenje flash memorije do 64 GB za spremanje programa i podataka. A, opremljen je i 40-polnim GPIO zaglavljem od 40 pina, baš kao i Raspberry Pi 4, koji omogućava povezivanje više senzora i podržava SPI i I2C protokole. Ima ugrađeni wifi za povezivanje s kućnom mrežom, a može se napajati i mikro USB-om s prijenosnog napajanja ili zidnog napajanja.

Kako dalje napredujete s IoT dizajnom prototipa, u toku razvoja možete zastati na trenutak I uporediti dobivene performance sa dizajniranom namjenom. U ovoj fazi

možete razmotriti vaš dizajn I rezultat prototipa uređaja, ugrađeni izbor softvera i odabir usluga i aplikacija za prenos podataka.

Možete periodično procijeniti svoje prototipove prema funkcijskim i nefunkcionalnim zahtjevima, uključujući performanse, pouzdanost i sigurnost, te ponovno pregledati te izbore po potrebi.

Hardverski zahtjevi za implementaciju komercijalnog IoT projekta

Nakon što ste razvili svoj prototip, na red dolazi obezbjeđenje hardvera za vaše kompletno IoT rješenje.

IoT uređaji su visoko specijalizirani. Oni su primarno dizajnirani za rad u vrlo specifičnim okruženjima.

Hardver za IoT projekte uvelike varira.

Iako se možete prototirati s generičkim hardverom koji lako možete nabaviti (u radnjama ili online), na kraju možete krenuti prema dizajnu i razvoju prilagođenih PCB-a i komponenti prilagođenih potrebama vaših IoT rješenja.

Prilikom planiranja hardvera za vaš projekat, potrebno je da razmotrite slijedeće hardverske zahtjeve:

- Sigurnosni zahtjevi;
- Jednostavnost razvoja;
- Zahtjevi za prikupljanje, obradu i pohranu podataka;
- Zahtjevi za povezivanje;
- Zahtjevi napajanja;
- Fizički dizajn uređaja;
- Zahtjevi troškova.

Krenimo redom.

Sigurnosni zahtjevi

Sigurnost je kritični element unutar IoT-a. Ovaj zahtjev je nužan za razmatranje u svim fazama dizajna i razvoja. Cjelovitost podataka i sigurnost koje je prikuplja bilo koji uređaj moraju ostati netaknuti, čak i za vrijeme izrade prototipa. Sigurnosni zahtjevi odnose se na same IoT uređaje, vašu mrežu te na cloud, mobilne i web usluge.

Srodni sigurnosni zahtjevi uključuju:

- Osiguravanje da svaki uređaj ima dovoljno snage i memorije za obradu kako bi mogao šifrirati i dešifrirati podatke i poruke brzinom kojom se šalju i primaju;
- Osiguravanje da ugrađene biblioteke softverskog razvoja podržavaju sve mehanizme autorizacije i kontrole pristupa koji se koriste za provjeru autentičnosti s upstream uslugama i aplikacijama;
- Odabir usvajanja komercijalnih uređaja koji implementiraju protokole za upravljanje uređajima za sigurno registriranje novih uređaja jer su dodani u mrežu kako bi se izbjeglo podmetanje (eng. spoffing) i onih koji uključuju mogućnost firmvera za podršku sigurne nadogradnje za zrak zbog sigurnosnih zakrpa.

Jednostavnost razvoja

Dok ste pravili prototip, lakoća (jednostavnost) razvoja zahtjev visokog prioriteta, iz razloga što tako možete brzo i jednostavno pokrenuti svoj IoT uređaj, snimiti podatke i komunicirati s drugim uređajima i oblakom.

Međutim, kada razvijate svoj projekat takođe morate da razmislite I o dodatnim pitanjima kao što je dostupnost komponenti, dostupnosti i kvaliteti API dokumentacije, razvojnih alata i podrške koje nudi proizvođač hardvera ili razvojna zajednica.

Odaberite uređaje koji se brzo i lako programiraju i lako reinstaliraju, kao i da imaju sposobnost da se lako lansiraju, bez potrebne ili minimalne konfiguracije na uređaju, kako biste smanjili frustraciju i uštedjeli vrijeme dok razvijate svoje IoT rješenje.

Zahtjevi za prikupljanje, obradu i pohranu podataka

Broj povezanih senzora, rezolucija snimljenih podataka i brzina kojom se podaci uzimaju određuju volumen podataka koji se obrađuju, što utiče na potrebe obrade i pohrane podataka.

Količina podataka koju je potrebno zadržati na uređaju zavisi o učestalosti povezivanja uređaja za prenos podataka prema bazama koje se nalaze na serveru.

Žičani, uvijek povezani uređaj koji je instaliran u pametnoj zgradi, a koji usmjerava male količine neobrađenih podataka direktno na visoko dostupan server, zahtijevat će manju moć obrade podataka i pohranu u odnosu na uređaj koji treba obraditi veliku količinu podataka. Za uređaj koji se povezuje samo svakih nekoliko sati radi uštede energije trebat će više memorije za pohranu podataka u međuvremenu.

Zahtjevi za povezivanje

Zahtjevi za povezivanjem za bežično umrežavanje uključuju radni raspon, koliko će signala trebati prenijeti, te predviđenu količinu i brzinu podataka za prijenos. Uzmite u obzir toleranciju grešaka i mogućnost da uređaj ponovno poveže i pokuša ponovo slati podatke nakon što je isključen.

Vaš hardver možda ima integriranu mrežnu povezanost kao što je Bluetooth ili wifi, ili će ovu mogućnost možda trebati dodati ploču ili modul za proširenje. Vanjski modul koji se može nadograditi može pružiti veću fleksibilnost jer imate mogućnost isprobavanja različitih modula kako biste procijenili njihov raspon i potrošnju energije.

Zahtjevi napajanja

Mnogi drugi zahtjevi, uključujući potreban broj senzora i brzinu mrežnog prijenosa, utjecati će na potrebe napajanja uređaja. Razmislite hoće li vaš uređaj biti ožičen za napajanje ili vam treba prijenosni izvor napajanja, poput baterije ili superkapacitator. Ako vam je potrebno prijenosno napajanje kao što je baterija, morate znati veličinu, težinu i zahtjeve za kapacitetom, kao i da li mora biti punjiva, zamjenjiva ili odbačena nakon što baterija umre. Ako je uređaj punjiv, koliko često ga treba puniti i na koji način?

Zahtjevi za fizički dizajn uređaja

Fizički zahtjevi za dizajn uređaja uključuju izgled i veličinu uređaja.

Na primjer, trebaju se uzeti u obzir i okolišni uvjeti u kojima će se uređaj instalirati, treba li vodootporno ili robusno kućište? Na primjer, uređaj koji je postavljen na donjoj strani kamiona, kao dio aplikacije za nadzor voznog parka, trebao bi biti oklopljen kako bi se osiguralo da i dalje radi u oštrim uslovima i morao bi biti vodootporan i otporan na prljavštinu, udarce i vibracije.

Zahtjevi troškova

Trošak hardvera uključuje početnu potrošnju hardvera i pridruženih komponenti (poput bilo kojeg senzora), kao i njihove tekuće troškove rada, poput troškova napajanja i održavanja u obliku zamjene istrošenih dijelova ili neispravnih komponenti.

Također razmotrite moguće naknade za licenciranje nekih komponenata ili upravljačkih programa uređaja.

Kupnja komercijalno dostupnih razvojnih ploča ili SBC-ova na mreži može biti ekonomičnija od izrade ploča po mjeri. Kako razmjenjujete svoju IoT mrežu s mnogim uređajima, namjenski hardverski uređaji mogu postati mudrija alternativa.

Zaključak

Svaka aplikacija i situacija su različiti. Ne postoji pristup "jedna veličina odgovara svima " za odabir hardvera za IoT projekte.

Usvajanje komercijalnog hardvera poput mikrokontrolera ili računara s jednim pločom koji se temelji na standardima može uštedjeti vrijeme i troškove u ranim fazama razvoja, bez žrtvovanja fleksibilnosti.

Ono što naučite u fazi prototipiranja može vam pomoći donošenju kritičnih odluka o dizajnu hardvera kasnije prilikom implementacije vašeg IoT rješenja.

3. Komponente IoT hardvera

Iot Starter Kits; Profesionalne IoT platforme

IoT Starter Kits

Nakon što ste saznali šta sve trebate da uzmete u obzir prilikom planiranja hadrvera za vaš IoT projekat, sigurno ste se zapitali ok, odakle da počnem.

Do sada ste već napravili plan vašeg IoT projekta, definsali ciljeve, došli ste do tačke kada trebate odrediti koji vam je konkretan hardver potreban za vaš projekat.

Jedan od prvih koraka koji vam možemo preporučiti jeste da prvi korak u razvoju vašeg IoT projekta bude nabavka IoT početnog seta (eng. IoTStarter Kits).

Zašto Starter Kits?

Za razvoj prototipa vašeg IoT projekta potrebno je da budete zaista sigurni da će vaš koncept stvarno raditi. IoT početni setovi pomažu vam da vidite što je moguće i najbolje od svega. Oni su spremni izvan okvira, tako da možete započeti s razvojem IoT aplikacija za osjetljivost na temperaturu, kretanje / udar, blizinu i izvještavanje o otvaranju / zatvaranju vrata.

Kako bi vam olakšali izbor IoT Starter Kits, u nastavku se nalazi pregled sedam najpopularnijih setova sa početka 2020. godine sa opisom njihovih najznačajnijih karakteristika.

Provjerite ih detaljno!

1. MakerFocus development board kit

MakerFocus je poznat po proizvodnji hardverskih uređaja s kvalitetnom i snažnom tehničkom podrškom. Brojni korisnici kupuju ovaj proizvod zbog kvalitete i jamstva koje nudi. Iz tog razloga, postao je 1. na našem popisu.

Ovaj je komplet uglavnom certificiran od strane Microsofta Azure koji osigurava sigurnost i brzo se povezuje.

Ovaj komplet može se koristiti kao dimni alarm, kamera, olovka za snimanje i timer. Također možete povezati s nekoliko drugih alata kao što su industrijski alat, sustav zaključavanja vrata, hotelski panel i stroj za rezanje aluminija.

To je zapravo uređaj veličine dlana koji ima visok stupanj dovršenosti i skalabilnosti. Kôd možete preuzeti u SDK formatu i implementirati na IoT uređaje za upotrebu u brojnim aplikacijama.

MakerFocus komplet markiran sadrži sljedeće komponente:

- Glavno jezgro
- USB kabl
- Mount
- DuPont line
- Naljepnice i
- Priručnik

Sve u svemu, performanse su dobre i zadovoljavaju osnovne potrebe DIYera. Sadrži priručnik koji upućuje korisnike na IOT i njegove radne modele.

Prednosti ovog kompleta su u tome da je vrlo ekonmičan, da obezbjeđuje korisničke usluge visokog standard I da ima dobra uputstva za upotrebu.

Nedostaci su mu u tome da Ne nudi jamstvo I da je malo kompliciran za početnike.

2. Imp. Explorer Kit

Drugi na listi je Electric imp brend. Kupcima nudi najbolje usluge proizvoda od ostalih spomenutih na popisu 7. Dizajn ovog IoT početnog kompleta očekuje se da će u početku biti vrlo osnovni.

To je jedan od najboljih startnih kompleta koje izdaje električni impuls koji može osjetiti i kontrolirati hardverske uređaje. Također možete potaknuti djecu na zanimljive projekte na znanstvenom sajmu koji će u budućnosti imati velike zahtjeve.

Njegova prednost je u tome što vam treba svega nekoliko minuta za postavljanje, instaliranje i povezivanje sa svijetom mogućnosti putem IOT-a.

Do sada su njegove primjene ograničene na nekoliko oblasti. Komplet sadrži USB, RGB LED, baterije i zaglave sustava za izradu projekta. Ima širok spektar integracija usluga u oblaku prikupljanjem podataka o okolišu za:

- Temperatura
- Vlažnost
- Akcelerometar i
- Pritisak zraka

IOT komplet sadrži sljedeće komponente koje su uredno upakirane u kartonsku kutiju dimenzija 4,3 * 3,3 * 1,5 inča su:

- Kit za programere

- IOT Wi-Fi modul
- USB kabl
- Napajanje
- RGB LED i
- baterije

Njegove prednostu su da je jednostavan za instalaciju, da nudi visokokvalitetne standardne usluge kupcu I da je vrlo jeftin.

Ove performase su razlog tome da su njegovi glavni nedostaci u tome da ima lošiju kvalitetu izrade i da nije kompatibilan s puno elektroničke opreme.

3. Particle Maker kit for learning IoT

Broj 3 dolazi od Brenda Particle Maker. Ova je marka poznata po dizajniranju vrhunskih elektroničkih startnih kompleta i nudi dobru korisničku uslugu.

Iako je cijena proizvoda skupa, možete započeti s dizajnom IOT projekata sa svim potrebnim komponentama i dodacima koji su dostupni u Particle Maker kompletu.

S ovim početnim kitom možete naučiti i dizajnirati 4 dokumentirana projekta za izradu prototipa s dodatnih 250 projekata. Usluge u oblaku su pristup između web-a i hardverske opreme. Ugrađene integracije putem web-uređaja podatke prenose u Google Cloud ili druge usluge.

Uz dijelove se nalazi priručnik s uputama za rukovanje hardverskim dijelovima i postupcima sastavljanja.

Ovaj početni set Particle IOT sadrži sljedeće komponente:

- Jumper žice
- LED diode
- otpornici
- kondenzatori
- tranzistori
- ploča
- USB kabl
- Čip kontrolera
- SD kartica i
- Napajanje

Njegove prednosti su u njegovoj prenosnoj prirodi, da je vrlo ugodan za korištenje I da vam treba Samo nekoliko minuta postupka instalacije.

Nedostaci su mu da je lošije kvalitete I da je malo skuplji u odnosu na predhodne pobrojane.

4. AT&T IoT starter kit powered by AWS

T&T je multinacionalna kompanija koja dizajnira jedinstvene proizvode na području elektronike i tehnologije. Ovaj poznati brend zalaže se da kupcima pruži visokokvalitetne usluge proizvoda te je na našem popisu bio broj 4.

Ovaj startni set sadrži mikrokontroler ploču, adapter, SD karticu, SIM karticu, USB kabal i žice za povezivanje. Slično je Arduinoj ploči, ali ne može funkcionirati u svim operacijama koje Arduino može obavljati.

Hardverska platforma omogućava vam razvijanje okruženja temeljenog na Cloud-u putem otvorenog koda SDA ili JTAG veze. Sadrži elemente potrebne za prikupljanje podataka, povezivanje s AT&T mrežom za pohranu i analizu IOT uređaja.

Također omogućuje dizajnerima da razviju i prototipiraju IoT uređaje povezane na stanicu uzimajući u obzir sljedeće sadržaje:

- Upravljačka ploča
- Stanični štit
- SIM kartica
- Memorijska kartica
- USB kabl
- Napajanje
- Spajanje žica i
- Priručnik s uputama

Prednosti ovog starter kit-a je da je vrlo pouzdan, da ima prenosni dizajn, ima dobar priručnik i kompatibilan s Raspberry Pi.

Njegovi nedostaci su da je suviše skup za kupovinu, a mogu se pojaviti i problem sa povezivanjem.

5. SparkFun IoT starter kit – blynk board

SparkFun starter set sa Blynk pločom jeodličan način rada u svijetu IOT alata bez prethodnog znanja o programiranju.

Važna je prepruka da se u radu sa ovim kompletom bolje upoznate o radu blynk boarda i njenoj upotrebi kako bi bez problema započeli rad na IoT uređajima.

Lemljenje također nije potrebno. Početni setovi obično dolaze s potpuno programiranim i pretplatničkom karticom za povezivanje s upravljačkom pločom. Izvrsno podržava Android, IOS uređaje i nadgleda vremenske uvjete, kontrolira LED-ove sa vašeg pametnog telefona.

Da bi uređaj radio, jednostavno se povežite na Wi-Fi signal i koristite ga na odgovarajući način. Također, slijedite upute date u priručniku koji objašnjava rad hardverskih uređaja i 14 IOT projekata korak po korak.

U radu na vašem IoT projektu korištenjem SparkFun starter kit-a, možete koristiti slijedeće komponente:

- LED diode
- otpornici
- kondenzatori
- Jumper žice
- sonde
- Napajanje
- USB kabl
- Upravljačka ploča i
- Korisnički vodič

Kad govorite o performansama, sjajan je zapravo zbog nebrojenih aplikacija u industriji. Ako tražite način da se upoznate s IoT uređajima, pokušajte s ovim SparkFun starter setovima.

Ovak komplet ima prednost u tome da ne koristi kablove, da je vrlo ekonomičan, a lemljenje nije potrebno.

Nedostaci su mu da mu je kvaliteta izrade lošija I da nije mnogo fleksibilan u poređenju sa drugim kompletima.

6. Adafruit Microsoft Azure IoT starter kit

Konačno, Adafruit Microsoft Azure starter kit posljednji je na našem popisu. IOT starter set proizvodi NKC. Ova popularna marka nudi veliki odjeljak Arduino-Raspberry Pi ploče i druge elektroničke uređaje.

Dijelovi u kompletu izrađeni su od visokokvalitetnih materijala. Zbog toga je cijena vrlo visoka u usporedbi s ostalim IOT starter setovima.

Ovaj vrhunski početni set uključuje unaprijed lemljene komponente poput glava za slaganje i servo motora. Kompatibilne su, pouzdane i brze ploče s ugrađenim USB-om i punjenjem baterije.

Nove dizajnerske karakteristike su prijenosne s mikrokontrolerima i omogućuju rad na različitim aplikacijama poput ispitivanja automobila, zaključavanja vrata i mnogih drugih.

Za izradu takvih zabavnih projekata potrebne su vam navedene komponente koje su dostupne u ovom početnom kompletu Adafruit IoT:

- USB kabl
- otpornici
- LED diode
- Piezo zujanje
- Sklopke
- Slaganje zaglavlja
- SPI senzor
- Mikro servo
- PIR osjetnik
- Vibracijski prekidač i
- Magnetski kontaktni prekidač
- Ploča pune veličine
- RGB senzor u boji i
- M / M-kratke žice

Njegova prednost je u kvaliteti, prenosivošću, i jednostavnošću rukovanja.

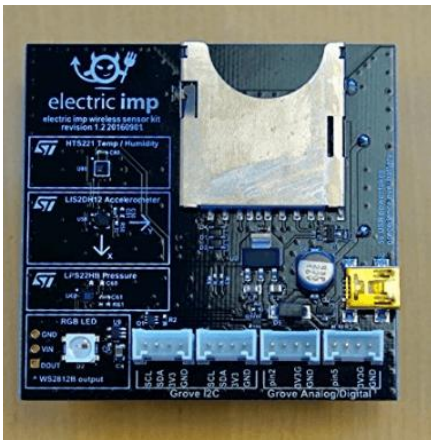
Nedostatak? Cijena. Da i baterije nisu uključene.

Kako izgledaju ovi startni kompleti pogledajte u narednom prikazu.

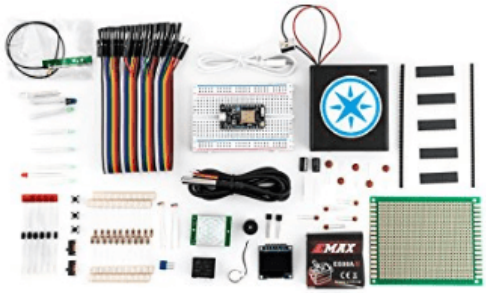
Prikaz: Fotografije odabranih IoT Starter kits

MakerFocus

Imp. Explorer Kit



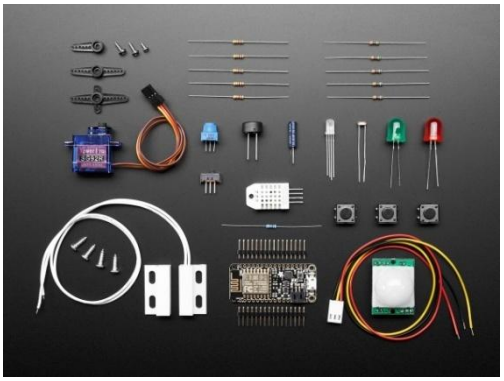
Particle Maker



AT&T IoT starter kit

SparkFun IoT

Adfruit Microsoft Azure IoT



Profesionalne IoT platforme

U predhodnoj sekciji ste se mogli upoznati sa hadrverom koji vam stoji na raspolaganju za razvoj prototipa vašeg IoT projekta.

Kao što ste mogli vidjeti svaki hardver se sastoji od centralne matične ploče /kontrolera i niza senzora pomoću kojeg vaš ioT uređaj prikuplja I prenosi podatke do vaše aplikacije.

Predstaavljeni hadrver je uglavnom komercijalni hadrver koji se lako može kupiti u prodavnici ili online.

Ovaj hadrver možete koristiti ne samo za vaš prototip već I za vaše finalne IoT projekte. Ali za IoT koji se koristi u industriji sve više je u primjeni industrijiski IoT za koje brojne kompanije razvijaju specijalizovani hadrver ili profesionalne IIoT platforme.

Na tržištu industrijske IoT platforme postoje mnogi dobavljači koji nude nevjerojatno slične mogućnosti i načine primjene. A niti jedan se od njih nije dovoljno diferencirao u ovom trenutku da bi bio jasan lider na tržištima u nastajanju.

Kako bi vam pomogli da se bolje upoznate sa IIoT platformama poslužit ćemo se Gartnerov čarobni kvadrantom (Gartner Magic Quadrant) koji je trenutno najbolji alat za procjenu bilo koje digitalne platform ili alata koji se koristi na tržištu (ne samo za IoT već I za bilo koji drugu digitalnu uslugu).

Od 2018. Godine Gartner objavljuje Magic Quadrant za Industrijske IoT platforme. Prema podacima za 2019. Godinu (iz maja 2019.) Gartner je identifikovao veliki broj IIoT platform koji nam puno olašava zadatak da vam predstavimo hadrver koji je trenutno najzastupljeniji u profesionalnim IoT projektima.

S obzirom na iscrpljeno i prenapučeno tržište te sve veći potencijal IIoT-a da izvlači vrijednost iz podataka, smanjuje troškove, poboljšava poslovanje i predstavlja nove poslovne modele, preporučuje se da dovoljno vremena posvetite istraživanju platform koja najviše odgovara vašim potrebama odnosno potrebama određene industrije za koju razvijate projekat.

IIoT platforme se razlikuju od naslijeđene operativne tehnologije (OT) u industrijskim okruženjima. Omogućuju isplativije prikupljanje većih količina velikih brzina, složenih strojnih podataka s umreženih IoT krajnjih točaka. Oni poboljšavaju uvid kroz specijalizirane analize podataka i omogućuju akcije, a poboljšavaju vizualizaciju podataka. Za industrijska poduzeća "neostvareno obećanje" IIoT-a je spojiti prednosti OT-a i IoT-a za "poboljšano prikupljanje podataka, praćenje stanja i vrhunsku analitiku", rekao je Gartner. "Zajedno će ove kombinirane ponude proširiti i na kraju zamijeniti naslijeđene sisteme upravljanja."

Prikaz: Gartnerov magični kvadrant za IIOT Platforme za 2019. godinu

Gartner je u svom izvještaju jasno pokazao da još uvijek nema tržišnog lidera na polju Industrial IoT platformi. Pa ipak, mnogi ozbiljni igrači su usli u utakmicu. Trenutno na tržištu najbolju poziciju imaju PTC, Software AG I Hitachi

Ova trojica su ocijenjena kao "vizionari" u ocjeni, radi cjelovitosti svojih IIoT strategija, kao i zbog sposobnosti izvršenja na njima. Ostatak je izgledao manje stabilno, igrajući se kao "nišni" igrači, a SAP je trenutno potpuno odustao od takmičenja zbog zaustavljanja podrške kanala svoje ko-brendirane IIoT platforme.

Gartner je rekao o njemačkom Software AG-u, koji svojim platformama Cumulocity IoT osigurava infrastrukturu za brojne IIoT platforme većih marki (isključene iz Gartnerove recenzije) da se odlikuje snagom tehničkog rješenja, aktivnošću kanala, i dobrim dosadašnjim rezultatima.

Istaknuo je svoj rad s industrijskim kupcima, uključujući Nordex, Entrematic i SIAD, kao i s dobavljačima industrijskih IoT rješenja i proizvodnim skupinama, uključujući Dürr i CERTUSS. "U svim slučajevima poboljšanja operativne efikasnosti ili upravljanja imovinom kupaca postignuta su primjenom rješenja Cumulocity IoT."

Slično tome, ThingWorx PTC-a hvaljen je zbog svog "dugogodišnjeg iskustva" i "globalnog ekosistema", kao i zbog reputacije i rezultata ulaganja. "PTC održava globalnu prodajnu silu i indirektni kanal preprodavača širom svijeta", navedeno je. U međuvremenu, Hitachijeva platforma Lumada nazvana je „cjelovitim cjelovitim rješenjem koje zadovoljava lokalne i oblačne instalacije u industriji koja intenzivno koristi kao što su proizvodnja, transport, energija i komunalije“.

Top 10, redom, navedeni su u nastavku. Potpuni opis tri glavne platforme IIoT nalazi se na dnu. Ovdje je veza s Gartnerovim čarobnim kvadrantom za industrijske IoT platforme.

1. Software AG (Cumulocity IoT)
2. PTC (LiveWorx)
3. Hitachi (Lumada)
4. Accenture (CPaaS)
5. Altizon (Datonis IIoT)
6. Egzosit (Murano IIoT)
7. IBM (Watson IoT)
8. Litmus Automation (Loop IoT)
9. Oracle (Oracle IoT Cloud Service)
10. Davra (Davra IoT Platform)

Novi igrači na polju IIoT u 2019. godinu uključuju Davra, Eurotech, Exosite, GE Digital, Litmus Automation i ROOTCLOUD. Exosite je na petom mjestu sa Altizonom i IBM-om. Litmus Automation pojavljuje se u zajedničkom osmom, s Oracleom. Davra je na desetom mjestu.

Gartner je rekao da neusklađenost ne isključuje izvrsnost u IIoT prostoru, nužno ili razmatranje poduzeća. Ostali značajni uglednici s IIoT tržišta uključuju ABB, Alibaba, AWS, Huawei, Microsoft, Schneider Electric i Siemens.

Alibaba, AWS, Huawei. Microsoft nije dostupan kao lokalna implementacija osim implementacije u Cloud-u. ABB-ove mogućnosti AT IoT i EcoStruxure IoT ne smatraju se samostalnom horizontalnom platformom IIoT koja se može prodati. U međuvremenu,

Siemensova platforma MindSphere IoT je isključena jer koristi usluge više pružatelja usluga oblaka i drugih partnera u svojoj ponudi.

1. Softver AG / Cumulocity IoT

Osnovana IIoT platform kompanije Software AG je Cumulocity IoT, koja se sastoji od Cumulocity IoT Core i Cumulocity IoT Edge. Softver zajedno omogućuje upravljanje uređajima, pametna pravila, kokpit i unaprijed konfigurirane IIoT aplikacije i opcionalno integrirane komponente kao što su analitika u stvarnom vremenu, integracija poduzeća i oblaka te upravljanje podacima i API-jem.

Platforma je dostupna u Cloud-u i u "prostoriji" uključujući hibridni rubni oblak i može se koristiti samostalno ili u kombinaciji s portolijem aplikacija za digitalnu transformaciju koje posjeduje kompanija Software AG. Mogućnosti upravljanja podacima, analitikom i integracijom postaju dostupne pomoću alata kao što su webMethods, Trendminer, Zementis, Apama i Built.io, itd.

Software AG je izoštrio fokus na IIoT tržištu uspostavljanjem zasebnog segmenta digitalne poslovne platforme i IoT izvještajnog segmenta. To ubrzava rast IoT poslovanja u cjelini i IoT centar izvrsnosti kao sloj globalnog prodajnog tima. U 2019. godini Software AG je uveo i zasebnu poslovnu jedinicu posvećenu IoT-u i analitikama. Uz napore u izravnom kanalu, putem prodavačkog kanala od preko 55 prodavača, Software AG od ovih partnera ostvaruje 50% prihoda od svoje IIoT platforme. "

2. PTC / ThingWorx

Platforma kompanije PTC ThingWorx dostupna je je kao lokalna implementacija (u prostoriji), Cloud opciji i hibridnoj opciji i koristi, po potrebi, kao poboljšanje za postojeće Cloud IIoT platforme kao što su Microsoft Azure IoT Hub, AWS IoT i FactoryTalk Rockwell Automation isl.

Snaga ove platform leži u dugogodišnjem iskustvu s imovinom na vertikalnim tržištima i teži se fokusiranju na nadzor imovine, prediktivno održavanje i rješenja korištenja imovine. Da bi razvio ta rješenja i poznavanje industrije, PTC je razvio globalni ekosustav tehnoloških partnera fokusiranih na IIoT, davatelja rješenja i globalnih integratora sustava.

Konačno, ThingWorx je jedna od najpoznatijih IoT platformi na tržištu koja se konstantno razvija. Promatrani i provjerljivi slučajevi industrijske upotrebe uključuju nadgledanje imovine i predviđanje održavanja više imovine na terenu, poput automobilskih voznih parkova i povezanih industrijskih proizvoda, te proizvodne radnje, kao što su roba i roba upakirana s potrošačima. "

3. Hitachi / Lumada

Platforma Hitachi Lumada može ponuditi različite vrste IoT usluga u Cloud-u, posebno na ključnim tržištima poput pametnih gradova i teških industrijalaca. Ona nudi cjelovito rješenje koje zadovoljava lokalne instalacije i vrste oblaka za industrije koja intenzivno koriste imovinu poput proizvodnje, transporta, energetike i komunalnih usluga.

Nadalje, Hitachi je razvio svoju distribuciju digitalnih blizanaca pod nazivom "Asset Avatars". Lumada Asset Avatari smatraju se digitalnim blizancima male vjernosti jer je funkcionalnost usmjerena na nadzor imovine i značajke upozoravanja.

Jedna od glavnih Hitachi-jevih strategija izlaska na tržište je prodaja Lumade u okviru svojih podružnica kao rješenje bijelih okvira ugrađenih u ponudu podružnica. Primjer bi mogao biti Hitachi Suite za vizualizaciju koji pokreće Lumadin hibridni Cloudk i Edge computing koje je izuzetno efikasno za IoT aplikacije u oblasti Smart city.

4. Cloud IoT

Uloga računanja u oblaku u IoT; Prednosti

Uloga računanja u oblaku u IoT

Računanje u oblaku je često korišten prevod Cloud computing tehnologije koja sve više postaje nezamjenjiv dio digitalnih ekosistema organizacija.

Do sada ste već primjetili da smo do sada često spominjali Cloud servise kada smo govorili o IoT ekosistemu uopšte, pojedinom hardveru ili IoT platform. Zapravo Cloud sa svojim IoT servisima ima veliku ulogu u "demokratizaciji" IoT i njegovoj primjeni u razvoju pametnih gradova i kuća, pametnoj trgovini,pametnim fabrikama, povezanim automobilima i brojnim drugim oblastima koje vode stvaranju efikasnijeg I automatizovanijeg svijeta u kojem živimo.

Zašto je to tako?

Cloud servisi značajno olakšavaju trenutnu, na zahtjev, isporuku kompjuterske infrastrukture, baze podataka, pohrane i aplikacija potrebnih za obradu i analizu podataka koji su generirani kroz IoT uređaja.

Nije čudo da je 96% organizacija prihvatilo Cloud u jednom ili drugom obliku. A s pojavom servisa kao što suAmazon Web Services, Google Cloud Platform, Microsoft Azure i IBM Cloud, izgledi za rast IoT-a postaju još svjetliji.

Šta je Cloud computing?

Jednostavno rečeno, računalstvo u oblaku je isporuka kompjuterskih usluga - uključujući servere, pohranu podataka, baze podataka, umrežavanje, softver, analitiku i inteligenciju - putem Interneta („oblak") kako bi ponudili brže inovacije, fleksibilne resurse i ekonomiju razmjera.

Obično plaćate samo za usluge u oblaku koje koristite, pomažući vam da snizite troškove poslovanja, učinkovitije pokrenete svoju infrastrukturu i povećate razmjenu poslovanja.

Računarstvo u oblaku velik je pomak od tradicionalnog načina na koji poduzeća razmišljaju o IT resursima. Evo sedam uobičajenih razloga zbog kojih se organizacije okreću uslugama računanja u oblaku:

1. Cijena

Računalstvo u oblaku uklanja kapitalne troškove kupnje hardvera i softvera, postavljanje i pokretanje podataka na licu mjesta – vitrine pune servera, non-stop struja za napajanje i hlađenje te IT stručnjaci za upravljanje infrastrukturom.

2. Brzina

Većina usluga računalstva u oblaku pruža se samostalna usluga i na zahtjev, tako da se čak i ogromne količine računalnih resursa mogu predvidjeti u nekoliko minuta, obično uz samo nekoliko klikova mišem, što tvrtkama pruža puno fleksibilnosti i uklanjanju pritiska pri planiranju kapaciteta.

3. Globalna razmjera

Prednosti usluga računalstva u oblaku uključuju mogućnost elastičnog skaliranja. Kada govorimo u oblaku, to znači isporuku prave količine IT resursa - na primjer, više ili manje računalne snage, prostora za pohranu, propusne širine - tačno kad su potrebni, i s pravog geografskog položaja.

4. Produktivnost

Centri podataka (end. Datacenters) na licu mjesta obično zahtijevaju puno "stajanja i slaganja" - postavljanje hardvera, krpljenje softvera i druge dugotrajne poslove upravljanja IT-om. Računalstvo u oblaku uklanja potrebu za mnogim od ovih zadataka, tako da IT timovi mogu potrošiti vrijeme na postizanju važnijih poslovnih ciljeva.

5. Performanse

Najveće usluge računalstva u oblaku rade na svjetskoj mreži sigurnih data centara, koji se redovito nadograđuju na najnoviju generaciju brzog i učinkovitog računalnog hardvera. To nudi nekoliko prednosti u odnosu na jedan korporativni centar podataka, uključujući smanjene mrežne latencije za aplikacije i veću ekonomiju razmjera.

6. Pouzdanost

Računarstvo u oblaku čini sigurnosnu kopiju podataka, oporavak od katastrofe i kontinuitet poslovanja lakšim i jeftinijim, jer se podaci mogu smjestiti na više web lokacija mreže pružatelja usluga oblaka.

7. Sigurnosti

Mnogi pružatelji usluga oblaka nude širok skup politika, tehnologija i kontrola koje u cjelini jačaju vaše sigurnosno držanje, pomažući zaštititi vaše podatke, aplikacije i infrastrukturu od potencijalnih prijetnji.

Prednosti IoT Cloud Computing

Na temelju principa skalabilnosti i okretnosti, oblak se smatra revolucionarnom tehnologijom diljem svijeta. Cloud rješenja mogu katalizirati široko prihvaćanje IoT inicijativa. Evo nekoliko ključnih razloga zašto je oblak neophodan za uspjeh IoT-a.

1. Računarska snaga na daljinu

S brzim napretkom 5G mreža i brzg interneta uopšte, cloud tehnologija postaje sve popolarnija jer omogućava kompanijama pristup udaljenim računarskim uslugama klikom miša. Smanjenjem potrebe za održavanjem lokalne infrastrukture, cloud je omogućio organizacijama da nadiđu uobičajene aplikacije IoT-a (npr. U kućanskim aparatima) i otvorio vrata za veliku primjenu IoT-a na dosad neistraženim teritorijima.

2. Sigurnost i privatnost

Sve veće prisustvo IoT uređaja omogućilo je organizacijama automatizaciju zadataka, ali također postavlja ozbiljne probleme sigurnosti. Cloud sa svojim širokim rasponom kontrola na ovom mjestu predstavlja jedno efikasno i održivo rješenje. Cloud rješenja olakšavaju provedbu bezbjednosnih mjera sigurnosti - omogućuju organizacijama da usvoje robusne protokole šifriranja i provjere autentičnosti. Kao što ćemo viditi, pomoću vrhunskih Cloud rješenja moguće je upravljati i osigurati identitet korisnika koji pristupaju IoT uređajima.

3. Integracija podataka

Kako IoT nastavlja dobivati na značaju, institucije su počele eksperimentirati sa spojenim uređajima kako bi izvukle informacije u stvarnom vremenu o ključnim poslovnim procesima. Iako ti uređaji poboljšavaju operativnu efikasnost i optimiziraju troškove, oni također generiraju ogromne podatke koji su previše glomazni za obradu čak i za njihove analitičke platforme.

Rješenja utemeljena na oblaku dobro dolaze ovdje sustavi u oblaku s čvrstim mogućnostima integracije podataka koji obrađuju ogromne količine podataka koje potiču iz više izvora. Kao rezultat toga, podaci iz poslovnih sistema i povezanih uređaja pohranjuju se, obrađuju i analiziraju na istom mjestu.

4. Smanjenje barijera za ulazak

Inovatori u domeni IoT traže hosting rješenja bez puno komplikacija. Rješenja za hosting u oblaku sasvim su prikladna u takvim situacijama. Pomoću rješenja za hosting u oblaku, vi možete iskoristiti snagu udaljenih data centara u Indiji bez potrebe za instaliranjem skupog lokalnog hardvera i softvera. Osim toga, ove usluge u oblaku djeluju na modelu "plati koliko koristiš", gdje se korisniku naplaćuje prema resursima koji potroši. Kao rezultat tog, vi ste u mogućnosti izbjeći velike prethodne troškove.

S pojavom inovativnih rješenja za hosting u oblaku, barijera za ulazak za većinu tvrtki sa sjedištem u IoT-u postaje svedena na minimum, što im omogućuje besprijekornu provedbu velikih IoT inicijativa.

5. Kontinuitet poslovanja

Rješenja za računanje u oblaku poznata su po svojoj agilnosti i pouzdanosti. Usluge u oblaku sjede na vrhu mreže poslužitelja smještenih na više lokacija. Njihovi sustavi pohranjuju kopije vaših podataka u više podatkovnih centara u Indiji.

Kao rezultat ove suvišnosti, operacije zasnovane na IoT-u i dalje funkcioniraju čak i ako jedan od poslužitelja iz nekog razloga ili iz drugog razloga prestane s radom izvan mreže. Uz to, ne postoji rizik od gubitka podataka.

6. Komunikacija između uređaja

Osim što komuniciraju s nama, IoT uređaji i usluge trebaju se međusobno povezati. Cloud rješenja olakšavaju besprijekornu komunikaciju između IoT uređaja. Omogućuju mnoge robusne API-je, poput Cloudflare-a i Dropstr-a, i omogućuju interakciju između povezanih uređaja i pametnih telefona i na taj način utre put za rast povezanih tehnologija.

7. Uparivanje sa Edge computing

Edge computing ili praksa obrade podataka kraj ruba mreže na kojoj se podaci generiraju obično se koristi u IoT rješenjima kako bi se skratilo vrijeme odziva i ubrzala obrada podataka. IoT implementacije često koriste kombinaciju računalstva u oblaku i rubova kako bi dobili najbolje od oba svijeta.

Da biste to bolje razumjeli, razmislite o velikoj tvornici opremljenoj s hiljadama IoT senzora. U takvom scenariju ima smisla objediniti podatke blizu ruba prije nego što ih pošaljete u oblak na daljnju obradu. Time se smanjuju izravne veze koje dosežu do centraliziranog skladišta oblaka sprječavajući da se preoptereti.

Edge data centri ubrzavaju obradu podataka u stvarnom vremenu što donositeljima odluka omogućava brže djelovanje. Međutim, pristup samo za rubove ne nudi cjelovitu sliku poslovanja. U nedostatku oblačnog rješenja, tvornica će možda moći nadzirati svaki dio opreme pojedinačno, ali neće moći procijeniti kako ti uređaji rade jedan u odnosu na drugi. Samo optimalna kombinacija oblaka i ruba tvrtkama može pomoći da izvuku maksimalnu vrijednost iz svojih IoT inicijativa.

Cloud infrastruktura kao usluga

Računarstvo u oblaku stil je računalstva u kojem se skalabilne i elastične mogućnosti omogućene za IT pružaju kao usluga pomoću internetskih tehnologija.

Cloud infrastruktura kao usluga (IaaS) vrsta je usluge računalstva u oblaku.

Cloud IaaS je definiran kao standardizirana, visoko automatizirana ponuda, gdje računski resursi, nadopunjeni mogućnostima pohrane i umrežavanja, posjeduju pružatelja usluga i nude ih kupcu na zahtjev.

Resursi su skalabilni i elastični u skoro stvarnom vremenu, a mjereno upotrebom. Izloženo je izravno kupcu sučelja za samoposluživanje, uključujući internetsko korisničko sučelje i API. Resursi mogu biti pojedinačni ili višemjesečni, a domaćin im je davatelj usluga ili lokalno u korisničkom centru podataka.

Usvajanje Cloud IaaS često započinje modernim opterećenjima rada, naglašavajući produktivnost programera i poslovnu okretnost. Ali sve veća količina oblaka IaaS kupuje se za tradicionalne IT s naglaskom na smanjenju troškova, sigurnosti i sigurnosti. Infrastrukturni i operativni (I&O) voditelji obično vode izvor kada oblak IaaS treba koristiti za tradicionalno IT.

Nasuprot tome, izvor za moderno radno opterećenje obično upravljaju arhitekti poduzeća, vođe za razvoj aplikacija i vođe digitalnog poslovanja.

Mnoga poduzeća zahtijevaju davatelje usluga trećih strana kako bi efikasnije koristili Cloud IaaS.

Razumijevanje profila Cloud IaaS

Cloud IaaS pružatelji usluga koji ciljaju poslovne i srednje marketinške korisnike uglavnom nude visokokvalitetnu uslugu, s izvrsnom dostupnošću, dobrim performansama, visokom sigurnošću i dobrom korisničkom podrškom.

Kada čitate profile dobavljača, imajte na umu sljedeće:

- Svi bolji davatelji usluga imaju javnu IaaS ponudu u oblaku. Nekoliko njih također nudi industrijsku ponudu privatnog oblaka ili su objavile detalje takvih planova gdje je svaki kupac na standardizovanoj infrastrukturi i alatima za upravljanje oblakom. Iako ovo može, a može i ne nalikovati ni na usluzi javnih usluga u oblaku ni arhitekture ni kvalitete. Jedinstvena arhitektura i skup značajki i upravljanje oblakom u oblaku, kako za javni tako i za privatni oblak IaaS, kupcima olakšavaju kombiniranje i migraciju preko modela usluga kako to nalažu njihove potrebe.

- Svi veliki pružaoci IaaS ciljaju srednje tvrtke i poduzeća, kao i druge tvrtke koje koriste tehnologiju u mjerilu. Neki od pružatelja usluga mogu se usmjeriti na mala poduzeća i početnike. Međutim, zato što pružatelj cilja segment, ipak ne znači da je on dobro prilagođen potrebama tog segmenta. Nadalje, nemaju svi davatelji usluga za opsluživanje kupaca velikih razmjera, a neki imaju ograničenja kapaciteta u određenim regijama.
- Svi pružatelji usluga nude osnovni IaaS u oblaku - računanje, pohranu i umrežavanje resursa kao uslugu. Oni nude i dodatne mogućnosti s dodanom vrijednošću, posebno usluge cloud softverske infrastrukture - obično softvera i baza podataka kao uslugu - do i uključujući platformu kao uslugu (PaaS) mogućnosti. Ove usluge, zajedno s mogućnostima upravljanja IT operacijama (ITOM) kao usluga (posebno usluge povezane s DevOpsom), vitalni su diferencijal na tržištu, posebno za agilne kupce IT Mode 2. Iako svi davatelji usluga nude IaaS i PaaS, samo neki nude integrirane IaaS + PaaS; ti su pružatelji izričito naznačeni.
- Svi davatelji usluga tvrde da imaju visoke sigurnosne standarde. Međutim, opseg sigurnosnih kontrola kupcima znatno varira. Svi davatelji usluga mogu ponuditi rješenja koja će zadovoljiti zajedničke potrebe usklađivanja s propisima, osim ako nije drugačije naznačeno. Svi su veliki pružaoci pružaju relativno visoku razinu sigurnosti i opšte prihvaćenih praksi za sigurnost svojih skistema. Ali zapamtite da je sigurnost je zajednička odgovornost; kupci moraju ispravno konfigurirati kontrole i možda će trebati pružiti dodatne kontrole izvan onoga što nudi njihov pružatelj.
- Resursi infrastrukture obično se automatski ne kopiraju u više data centara, osim ako nije drugačije navedeno; kupci su odgovorni za vlastiti kontinuitet poslovanja. Neki pružatelji nude neobavezna rješenja za oporavak od katastrofe.
- Uopšte, cijena korištenja Cloud IaaS zavisi od veličine resursa koji se koriste i vrste licence. Većina velikih pružaoca usluga omogućava korisnicima korištenje ograničenih resursa besplatno.
- Pružatelji usluga obično mjere trošak strojeva virtualnih mašina najmanje svaki sat, dok neki nude i kraće korake mjerenja, što može biti isplativije za kratkoročne serijske poslove. Pružatelji usluga naplaćuju po VM, osim ako nije drugačije navedeno.
- Svi pružatelji usluga nude potporu za poslovnu klasu uz 24/7 korisničku službu, putem telefona, e-pošte i chata, zajedno s upraviteljem računa. Većina pružatelja usluga to uključuje svojom ponudom. Neki nude nižu razinu podrške prema

zadanim postavkama, ali omogućuju kupcima da dodatno plaćaju za podršku poslovne klase.

- Svi davatelji usluga potpisat će ugovore s kupcima, mogu fakturirati i objedinjavati račune s više računa. Svi pružatelji usluga nude i naplatu putem interneta i naplatu kreditnim karticama jer prepoznaju da poduzetnici kupuju ugovore i fakture. Neki će potpisati ugovore o "nula dolara" koji kupca ne obvezuju na određenu količinu.

Najbolji pružaoci usluga Cloud IaaS

Danas vrlo lako možete pronaći pružaoca usluga Cloud servisa. Možete odabrati nekog lokalnog pružaoca u Bosni i Hercegovini i da uporedite njegove usluge sa bilo kojim sličnim pružaocem usluga u svijetu.

Kako bi vam olakšali ovaj proces, koji može biti izuzetno komplikovan upoznaćemo vas sa trenutno vodećim globalnim pružaocima Cloud IaaS na svijetu.

Za to, naravno poslužićemo se magičnim kvadrantom koji objavljuje Gartner.

Važno je da znate da kada Gartner analizira pružaoca Cloud IaaS, oni prvo rezimiraju prirodu kompanije, njenoj globalnoj prisutnosti i razvijenosti industrijske Cloud IaaS ponude, popis ponuda, analiza odstupanja ponude od standardnih mogućnosti, mogućnosti pohranjivanja podataka, mreža za isporuku sadržaja (CDN), aplikacija PaaS (aPaaS) i upravljane usluge, ali ovo nije sveobuhvatan popis ponuda davatelja usluga, lokacije Cloud IaaS podataka u središtu podataka po zemljama, jezicima na kojima kompania posluje i jezicima u kojima se može provoditi tehnička podrška.

Ovo nisu jedine okolnosti u kojima on može biti koristan davatelj usluga, ali to su scenariji za koje, prema Gartnerovom mišljenju, pružatelj najbolje odgovara. Za sve dobavljače, preporučene uporabe specifične su za samoupravljajući oblak IaaS. Međutim, neki davatelji usluga također imaju upravljane usluge, kao i druge usluge oblaka i noncloud usluge koje se mogu koristiti u kombinaciji s oblakom IaaS. Tu se ubrajaju hibridni hostingi (kupci ponekad kombiniraju rješenja, poput potpuno samoupravljanog internetskog sloja na javnom oblaku IaaS, s upravljanim hostingom za aplikacijske poslužitelje i baze podataka), kao i hibridna IaaS / PaaS rješenja. Iako u ovom Čarobnom kvadrantu ne vrednujemo upravljane usluge, neintegrirani PaaS i slično, oni su dio ponuđačeve ukupne vrijednosti i spominjemo ih u kontekstu pružanja opširnijih preporuka rješenja.

Pogledajmo sada Gartnerov magični kvadrant za Cloud IaaS.

Prikaz: Gartner magični kvadrant za Cloud IaaS servise (Juli 2019)

Pogledajmo sada koje su to glavne snage i mjere opreza koje poduzimaju vodeći globalni pružaoci Cloud IaaS usluga.

Alibaba Cloud (Aliyun)

Alibaba Cloud, također poznat kao Aliyun na kineskom, pružatelj usluga usmjerenih na oblak sa sjedištem u Kini i podružnica je Alibaba Grupe. Osnovan 2009. godine radi pružanja usluga platforme tvrtkama e-trgovine Alibaba Grupe, Alibaba Cloud sada se prodaje tvrtkama širom svijeta. Ova Magična kvadrantna evaluacija usredotočena je na međunarodno poslovanje Alibaba Clouda sa sjedištem u Singapuru, a tehnička procjena obavljena je korištenjem međunarodne usluge.

Ponuda: Alibaba Cloud je integrirani IaaS + PaaS. Nudi Xen i KVM virtualizirani multitenant računar (Elastic Compute Service) s računalno neovisnom pohranom blokova (oblačni diskovi). Nudi i spremanje objekata (Alibaba Object Storage Service), CDN uslugu, uslugu kontejnera temeljenu na Dockeru (Cloud Container Service), unaprijed konfiguriranu infrastrukturu privatnog oblaka (Apsara Stack i ET Brain) i razne usluge na sloju PaaS uključujući obitelj usluga baze podataka (ApsaraDB).

Lokacije: Alibaba Cloud djeluje u više regija u Kini i dodatno ima prisutnost u SAD-u (Istočna i Zapadna obala), Njemačkoj, Australiji, Hong Kongu, Indoneziji, Japanu, Indiji, Maleziji, Singapuru, Ujedinjenim Arapskim Emiratima i Ujedinjenom Kraljevstvu. Ima lokalnu prodaju u SAD-u, Kini, Njemačkoj, Australiji, Japanu, Hong Kongu i Singapuru. Kineski servisni portal, dokumentacija i podrška nalaze se u Mandarini. Međunarodni portal, dokumentacija i podrška su na engleskom, mandarinskom i japanskom.

Profil usvajanja: Alibaba Cloud je trenutni vodeći tržišni udio u oblaku IaaS u Kini (42%) i posebno dobro se ponaša s kineskim digitalnim poduzećima i kineskim entitetima iz javnog sektora. U Kini Alibaba nudi privatne mogućnosti Cloud infrastrukture za kineske tvrtke koje žele hibridni oblačni model. Izvan Kine, unatoč najavljenim partnerstvima za 2018. godinu sa SAP-om i VMware-om, Alibaba Cloud najčešće koriste kupci Mode 2 u azijsko-pacifičkoj regiji koji traže platformu za agilno radno opterećenje.
Preporučena upotreba: prvo opterećenje digitalnog poslovanja u oblaku za korisnike koji su (1) sa sjedištem u Kini ili jugoistočnoj Aziji i žele iskoristiti odnos Alibaba Clouda s matičnom tvrtkom ili (2) treba locirati oblačnu infrastrukturu u Kini.

- **Prednosti**

Alibaba Cloud ima opsežan skup javnih IaaS + PaaS ponuda integriranih u oblak, što je po opsegu usporedivo s portfeljima usluga drugih globalno usmjerenih hipsterskih pružatelja usluga.

Alibaba Cloud vodeća je tržišna udjela za cloud IaaS u Kini, gdje ima pozitivne ocjene zadovoljstva kupaca, uz snažne veze s kineskim javnim sektorom. Kineske tvrtke vide Alibaba Cloud kao pokretač digitalne transformacije i kanal za početak ostvarivanja digitalnog prihoda.

Alibaba Cloud ima usku povezanost s Alibaba Group of Companies, što omogućava Alibaba Cloud da djeluje kao most u Kini za međunarodne kompanije, a most izvan Kine za kineske kompanije.

- **Mjere opreza**

Međunarodna ponuda Alibaba Clouda nema u potpunosti mogućnosti Kine, kao ni dubinu značajki svojih glavnih globalnih konkurenata (Amazon Web Services, Microsoft,

Google). U mnogim regijama određene su usluge možda dostupne samo kada se koriste određene vrste računalnih instanci.

Alibaba Cloud ostvaruje 90% svog prihoda u Kini i nije značajno povećao svoju klijentsku bazu izvan Kine. Alibaba ima ograničene mogućnosti u pogledu MSP ekosustava, integracije poslovnog softvera i operativnih alata treće strane; a mali globalni terenski timovi ograničavaju usvajanje izvan Kine.

Financijski gubici Alibaba Clouda sve su veći i mogu spriječiti kompaniju da nastavi ulagati u neophodna proširenja kako bi poslužila međunarodnim tržištima kao vodeći pružatelj hipersignalnih razmjera.

Amazon Web Services (AWS)

Amazon Web Services (AWS), podružnica Amazona, pružatelj je usluga usmjerenih na Cloud. Ušao je na tržište Cloud IaaS 2006. godine.

Ponuda: AWS je integrirani IaaS + PaaS. Njegov Elastic Compute Cloud (EC2) nudi višestruke multimedijske i jednostruke VM-ove koji se mjere do sekunde, kao i serverke koji su namjenjeni samo za jednog klijenta (Bare Metal Server). AWS-ovi hipervisori temelje se na Xen i KVM-u. Postoji višenamjensko spremanje blokova i datoteka, zajedno s velikim mogućnostima IaaS i PaaS. To uključuje pohranu objekata s integriranim CDN-om (Amazon Simple Storage Service [S3] i CloudFront), usluge Docker kontejnera (Amazon EC2 Container Service [ECS], ECS za Kubernetes [EKS] i Fargate) i „računarstvo bez servera“ usmjereno na događaje. (AWS Lambda). VMware nudi uslugu VMware Cloud Foundation u sklopu AWS podatkovnih centara (VMware Cloud on AWS). Podrška za poslovni nivo je dodatna. Ima SLA više domena s kvarom. Potrebe za smještajem zadovoljavaju se putem partnerske razmjene (AWS Direct Connect).

Lokacije: AWS grupira svoje data centre u regije, od kojih svaka sadrži najmanje dvije zone dostupnosti (data centri). Ima više regija diljem Sjedinjenih Država, kao i u Kanadi, Francuskoj, Njemačkoj, Irskoj, Ujedinjenom Kraljevstvu, Australiji, Indiji, Japanu, Singapuru, Južnoj Koreji, Švedskoj i Brazilu. Također ima jednu regiju posvećenu američkoj saveznoj vladi. Postoje dvije kineske regije - Peking (upravlja Sinnet) i Ningxia (upravlja Ningxia Western Cloud Data Technology [NWCD]) - za koje je potreban AWS račun za Kinu. Ima globalnu prodajnu prisutnost. Portal i dokumentacija dostupni su na engleskom, nizozemskom, francuskom, njemačkom, talijanskom, japanskom, korejskom, mandarinskom, portugalskom i španjolskom. Primarni jezici za podršku su engleski, japanski i mandarinski, ali AWS će se ugovorno obvezati na pružanje podrške na velikom broju drugih jezika.

Profil usvajanja: AWS snažno privlači kupce koji traže agilno poslovanje, ali često se bira i za tradicionalne stilove IT poslovanja. AWS je onaj koji se najčešće bira za strateško prihvaćanje širom organizacije. Napora na transformaciji najbolje je poduzeti u suradnji s SI.

Preporučene uporabe: Svi slučajevi upotrebe koji dobro funkcioniraju u virtualiziranom okruženju. Aplikacije koje potencijalno mogu izazvati virtualiziranje ili pokretanje u višenacionalnom okruženju - uključujući visoko sigurne aplikacije, strogo kompatibilne ili složene poslovne aplikacije (poput SAP poslovnih aplikacija) - zahtijevaju posebnu pozornost arhitekturi.

- **Prednosti**

Poduzeća preuzimaju veće godišnje financijske obveze i raspoređuju više kritičnih radnih zadataka na AWS-u nego kod bilo kojeg drugog pružatelja hiper-skala. Ovo govori o tome kako poduzeća vide AWS kao strateškog pružatelja usluge oblačne infrastrukture i usluga platforme u odnosu na ostale pružatelje usluga na tržištu.

AWS ima širi raspon korisničkih profila, u rasponu od startupa i malih i srednjih poduzeća (SMBs) do velikih poduzeća, od bilo kojeg drugog pružatelja usluga na ovom tržištu. Poduzeća koja koriste AWS imaju koristi od ranih usvajanja, koja pomažu gurati nove tehnologije u glavni tok, riskirajući takve usluge i olakšavajući im potrošnju i upravljanje kao rezultat.

AWS je najzreliji, za poduzeća korporativni pružatelj usluga, s najjačim uspjehom korisnika i najkorisnijim partnerskim ekosustavom. Dakle, pružatelj je izabran od strane ne samo kupaca koji cijene inovacije i koji provode digitalne poslovne projekte, već ih preferiraju i kupci koji migriraju tradicionalne podatkovne centre u oblak IaaS.

- **Mjere opreza**

AWS često objavljuje broj ostvarenih sniženja. Kupci tumače ove izjave kao široko primjenjive na usluge tvrtke, ali to nije slučaj. Na primjer, zadana i najčešće rezervirana pohrana za AWS-ovu računsku uslugu nije doživjela smanjenje cijena od 2014., unatoč padu cijena na tržištu sirovih komponenti.

AWS daje prioritet prvom tržištu na tržištu pružanja novih usluga i mogućnosti. Kao rezultat, spreman je pokrenuti usluge ili usluge siromašne značajkama bez duboke među-platformske integracije, što često odgađa budućnosti u budućnosti. Potraga da se prvo plasira na tržište ponekad rezultira uslugama za koje su potrebne godine značajnih inženjerskih ažuriranja.

Kako se ambicije čelnika Amazona šire na dodatna tržišta, upravni odbori za tvrtke u potencijalno ugroženoj vertikali usmjerili su svoje IT organizacije da izbjegnu uporabu

AWS-a tamo gdje je to moguće. To u konačnici može ograničiti uspjeh AWS-a u nekim vertikalima i utjecati na pridruženi ekosustav. IT vođe u tim vertikalama trebale bi razmotriti plan izvanrednih situacija za smjernice na razini odbora.

Google (Google Cloud)

Google je internetski davatelj tehnologije i usluga. Google ima ponudu aPaaS (aplikacijska platforma kao usluga) od 2008. godine, ali nije ušao u Cloud tržište IaaS sve dok Google Compute Engine nije predstavljen u lipnju 2012. (s općom dostupnošću u prosincu 2013.).

Ponude: Google Cloud Platform (GCP) kombinira IaaS ponudu (Compute Engine), aPaaS ponudu (App Engine) i niz dodatnih IaaS i PaaS mogućnosti, uključujući pohranu objekata, uslugu Docker kontejnera (Google Kubernetes Engine [GKE]) i "računanje bez serveraa" (Google Cloud Functions) na temelju događaja. Google također nudi GKE On-Prem (softver za lokalnu implementaciju), ponudu spremnika za poslovne primjene. Ima SLA više domena s kvarom. Potrebe za smještajem zadovoljavaju se putem partnerske razmjene (Google Cloud Interconnect).

Lokacije: Google ima više regija diljem SAD-a, kao i prisutnost u Belgiji, Japanu, Singapuru, Njemačkoj, Nizozemskoj, Ujedinjenom Kraljevstvu, Indiji, Australiji, Brazilu, Kanadi, Hong Kongu, Švicarskoj i Tajvanu. Google ima globalnu prisutnost u prodaji. Podrška je dostupna na engleskom i japanskom jeziku. Portal je dostupan na engleskom, nizozemskom, francuskom, njemačkom, talijanskom, poljskom, španjolskom, turskom, ruskom, portugalskom, korejskom, japanskom, mandarinskom, kantonskom i tajlandskom. Dokumentacija je dostupna na engleskom, njemačkom, japanskom i brazilskom portugalskom. Google upravlja regijama s zonama raspoloživosti, ali te zone mogu biti odvojene zgrade ili zasebne razine napajanja, hlađenja, umrežavanja i upravljanja.

Profil usvajanja: GCP se u početku obraćao kupcima Mode 2 s demonstriranom snagom povezanom s velikim podacima i drugim analitičkim aplikacijama, projektima strojnog učenja, aplikacijama koje su izvorne u oblaku ili drugim aplikacijama optimiziranim za operacije u oblaku. GCP također počinje privlačiti poduzeća s tradicionalnim radnim opterećenjem Mode 1 kao što je SAP.

Preporučene uporabe: Veliki podaci i druge analitičke aplikacije, projekti strojnog učenja, aplikacije koje se temelje u oblaku ili druge aplikacije optimizirane za operacije koje rade u oblaku.

- **Prednosti**

Google je iskoristio svoje interne mogućnosti inovativne tehnologije (npr. Automatizaciju, spremnike, umrežavanje) pružajući skalabilnu IaaS ponudu s PaaS mogućnostima usredotočenim na ekosustave otvorenog koda. Dok se u početku bave startup-ima koji stvaraju oblak, Google trenutno proširuje doseg na poslovne korisnike.

Google je različite tehnologije na prednjem rubu informatike, posebno u području analitike i Machine learning. To je natjeralo neka poduzeća da odaberu Googlea kao strateškog pružatelja usluga oblaka gdje su postavili aplikacije koje su usidrene od strane BigQueryja.

Google je inovirao programe koji pomažu kupcima u procesu transformacije operacija putem inženjerskog programa za pouzdanost kupaca. Program koristi pristup zajedničkim operacijama da nauči kupce da vode operacije na način na koji to rade Googleovi inženjeri za pouzdanost web mjesta. To može potencijalno privezati Google poslovnim kupcima.

- **Mjere opreza**

Google pokazuje nezrelost procesa i postupaka kad se bave poslovnim računima, što kompaniju ponekad može otežati. To se može pripisati njegovom početnom fokusu na tržište poduzeća. Nezrelost procesa najizraženija je u područjima kao što su pregovaranje ugovora, diskontiranje, licenciranje neovisnih dobavljača softvera (ISV), integracija s poslovnim sustavima i podrška. Google agresivno cilja na ove nedostatke.

Google ima mnogo manji bazen iskusnih partnera usluga profesionalnih usluga usmjerenih na MSP i infrastrukturu od ostalih dobavljača u ovom Čarobnom kvadrantu. Vlastite profesionalne usluge i dalje stječu privlačnost u pokretanju korisničkih implementacija. Neki potencijalni kupci smatraju da ta ograničenja ekosustava povećavaju migracijski rizik.

Googleova ukupna pokrivenost poduzeća iz perspektive prodaje i rješenja na terenu zaostaje za konkurentima. Nadalje, poduzeća se često žale na Googleovu nesposobnost da smisli odgovarajuća rješenja za potrebe poduzeća u suradnji s arhitektima rješenja.

IBM (IBM Cloud / bivši Bluemix)

IBM je velika, raznolika tehnološka kompanija s nizom Cloud povezanih proizvoda i usluga. Ponuda IBM Cloud utemeljena je na IBM-ovoj kupnji SoftLayera u 2013. godine i na njezinoj prethodnoj Bluemix ponudi.

Ponude: IBM nudi i računske resurse za multitenant i jednog korisnika (tenant) zajedno sa Bare metal service. Posjeduje S3 kompatibilnu pohranu podataka u oblaku. CDN integracija nudi se putem Akamai partnerstva. IBM Cloud nudi uslugu kontejnera na bazi

Open Container Initiative (OCI) (IBM Cloud Kubernetes Service), računanje bez servera (IBM Cloud Functions), aPaaS temeljeno na Cloud Cloudu i druge PaaS mogućnosti. IBM također nudi ponudu privatnog oblaka na bazi Kubernetes-a i spremnika (IBM Cloud Private). Upravljane usluge nisu obavezne. Potrebe za kolokacijom zadovoljavaju se putem partnerske razmjene (IBM Cloud Direct Link).

Lokacije: IBM ima SoftLayer infrastrukturu u više podatkovnih centara u SAD-u, zajedno s data centrima u Kanadi, Meksiku, Brazilu, Francuskoj, Njemačkoj, Italiji, Velikoj Britaniji, Nizozemskoj, Norveškoj, Australiji, Hong Kongu, Indiji, Japanu, Koreji, Švedska i Singapur. IBM nudi nekad Bluemix-ove usluge u Sjedinjenim Državama, Velikoj Britaniji, Njemačkoj, Australiji i Japanu. IBM ima globalnu prisutnost u prodaji. Nudi podršku na širokom rasponu jezika na kojima IBM posluje. Portal i dokumentacija dostupni su na engleskom, francuskom, njemačkom, talijanskom, portugalskom, španjolskom, pojednostavljenom kineskom, tradicionalnom kineskom, korejskom i japanskom.

Profil usvajanja: IBM apelira na svoje postojeće kupce koji imaju snažnu sklonost kupnji većine svojih tehnologija od IBM-a. Ti kupci uglavnom imaju slučajeve korištenja Mode 1. načina korištenja. Međutim, mogućnosti IBM Cloud infrastrukture mogu se koristiti i za dopunu ostalih IBM rješenja, poput Watson-a.

Preporučene upotrebe: IBM outsourcing ponude koje koriste bare metal servers kao hosting platformu, gdje kupac ima potrebu za dodatnim osnovnim Cloud IaaS. Infrastruktura se također može koristiti kao komponenta aplikacija izgrađenih na temelju mogućnosti IBM Cloud PaaS. Također bi se trebali uzeti u obzir u okolnostima koje zahtijevaju i API kontrolu nad skalabilnom infrastrukturom i poslužiteljima golog metala kako bi se ispunili zahtjevi za performanse, usklađenost s propisima ili licenciranje softvera.

- **Prednosti**

IBM ima vrlo veliku bazu korisnika s kritičnim aplikacijama koji počinju prihvaćati usluge oblaka. IBM je u dobroj poziciji da partner svojim uslugama pruža pomoć ovim kupcima kroz put transformacije oblaka.

IBM ima jaku marku i postojeće odnose s kupcima širom svijeta, a može ponuditi podršku na lokalnim jezicima, lokalne ugovore i naplate u lokalnoj valuti. IBM-ova baza strateških klijenata na outsourcing može pomoći u prihvaćanju IBM Cloud infrastrukture.

IBM je prešao na razmjenu poruka oko hibridnog i višesmjernog računanja, što ne dovodi izravno u pitanje mnoge pružatelje usluga u ovom Čarobnom kvadrantu. Umjesto toga, nudi mogućnosti i alate za poduzeća, omogućujući im da odaberu oblačno okruženje koje je najbolje za njihove specifične zahtjeve za aplikacije, pozicionirajući IBM Cloud kao nišu ili posebnost koja se nudi tijekom postupka odabira.

- **Mjere opreza**

IBM-ov projekt nove infrastrukture generacije (NGI) donio je postupna poboljšanja infrastrukturnih usluga koje su ranije bile pod kišobranom SoftLayer. Međutim, on nije postigao svoj temeljni cilj - proizvesti novi set cloud IaaS ponude temeljenih na načelima hipersvelike arhitekture. S obzirom na to, malo je vjerojatno da će IBM postati konkurentni IaaS javni pružatelj usluga oblaka.

Unatoč mnogim svjetskim data centrima, iskustvo IBM Cloud ostaje nepovezano jer su mnoge značajke dostupne samo na određenim lokacijama. Ovo i neobično korisničko iskustvo uzrokuju da IBM ima višu razinu nezadovoljstva korisnika u odnosu na ostale dobavljače u ovom istraživanju.

IBM ima manji ekosustav partnera koji pružaju susjedne alate (npr. Upravljanje troškovima, sigurnost, upravljanje). Uz to, ima manje partnerstva (u usporedbi s drugim davateljima usluga) s glavnim dobavljačima softvera (Microsoft, SAP, Oracle) koja bi mogla kulminirati uvođenjem u IBM Cloud.

Microsoft (Microsoft Azure)

Microsoft je veliki i raznovrstan dobavljač tehnologije koji se sve više fokusira na pružanje svojih softverskih mogućnosti putem cloud usluga. Microsoft je ušao na tržište IaaS u oblaku pokretanjem Azure Virtual Machines u 2012. (s općom dostupnošću u 2013.).

Ponude: Microsoft Azure integrira IaaS + PaaS. Nudi hiper-V virtualizirani multitenacijski računar (Azure Virtual Machines), kao i druge velike instance (poput SAP HANA). Postoji višenamjensko pohranjivanje blokova i datoteka, uz brojne dodatne IaaS i PaaS mogućnosti. To uključuje spremanje objekata (Azure Blob Storage), CDN, uslugu kontejnera utemeljenu na Dockeru (usluga Azure Container Service), uslugu paketnog računanja (Azure Batch) i "računarstvo bez poslužitelja" (funkcije Azure) na temelju događaja. Azure Marketplace nudi softver i usluge treće strane. Potrebe za smještajem zadovoljavaju se putem razmjene partnera (Azure ExpressRoute), poput onih iz Equinix-a i CoreSite-a.

Lokacije: Microsoft naziva lokacije podatkovnih centara Azure "regijama". Postoji više Azurnih regija u Sjedinjenim Državama, Kanadi, Ujedinjenom Kraljevstvu, Njemačkoj, Francuskoj, Australiji, Indiji, Norveškoj, UAE, Švicarskoj, Japanu i Koreji, kao i regijama u Irskoj, Nizozemskoj, Hong Kongu, Singapuru i Brazilu. Postoji i šest regija za saveznu vladu SAD-a; dvije su posvećene Ministarstvu obrane. (Dvije regije Azure Kine dio su zasebne usluge kojom upravlja 21Vianet grupa.) Microsoft ima globalnu prodaju.

Dokumentacija je dostupna na engleskom, francuskom, njemačkom, talijanskom, španjolskom, portugalskom (Brazil i Portugal), japanskom, korejskom i mandarinskom. Podrška i portal usluga dostupni su na tim jezicima, plus češki, nizozemski, mađarski, poljski, ruski, švedski i turski.

Profil usvajanja: Microsoft Azure privlači kupce Mode 1 i Mode 2, ali iz različitih razloga. Kupci prvog načina imaju tendenciju da cijene sposobnost korištenja Azure-a za širenje svojih infrastrukturno orijentiranih Microsoftovih odnosa i ulaganja u Microsoftove tehnologije. Kupci Mode 2 često cijene sposobnost Azurea da se integrira s Microsoftovim alatima za razvoj aplikacija i tehnologija, ili su zainteresirani za integrirane specijalizirane PaaS mogućnosti, kao što su Azure Data Lake, Azure Machine Learning ili ubrzavači rješenja Azure IoT.

Preporučene uporabe: Svi slučajevi upotrebe koji dobro funkcioniraju u virtualiziranom okruženju, posebno za Microsoftove organizacije.

- **Prednosti**

Kompanije koje su strateški opredijeljene za Microsoftovu tehnologiju općenito odabiru Azure za primarnog dobavljača IaaS + PaaS. Integrirano cjelovito iskustvo za poduzeća koja grade .NET aplikacije koje koriste Visual Studio i srodne usluge dok ih razmještaju u Azure nije nadmašljivo. Microsoft povećava ogroman prodajni domet i sposobnost ko-prodaje Azure s drugim Microsoftovim proizvodima i uslugama kako bi potaknuo usvajanje.

Azure pruža dobro integrirani pristup računanju rubova i Interneta stvari (IoT), s ponudama koje dosežu iz njegovog hiper-skali podatkovnog centra preko rubnih rješenja poput Azure Stack i Data Box Edge.

Mogućnosti Microsoft Azure postaju sve inovativnije i otvorenije, gdje je 50% radnog opterećenja temeljeno na Linuxu, zajedno s brojnim paketima aplikacija otvorenog koda. Microsoft ima jedinstvenu viziju budućnosti koja uključuje dovođenje tehnoloških partnera putem izvornih ponuda, prve strane poput VMware-a, NetApp-a, Red Hat-a, Cray-a i Databricks-a.

- **Mjere opreza**

Pitanja pouzdanosti Microsoft Azure-a i dalje su izazov za kupce, uglavnom kao rezultat rastućih bolova Azure-a. Od 2018. godine Azure je imao više incidenata na uslugu, uključujući značajne kvarove koji uključuju Azure Active Directory. Priroda mnogih tih kvarova je takva da kupci nisu imali kontrolu kako bi ublažili stanke.

Poduzeća često žale na kvalitetu Microsoftove tehničke podrške (zajedno s povećanjem troškova podrške) i arhitekata na terenu. To negativno utječe na zadovoljstvo kupaca, a usporava usvajanje Azure i samim tim na potrošnju kupaca.

Oracle (Oracle Cloud Infrastrucure)

Oracle je velika, raznolika tehnološka kompanija s nizom proizvoda i usluga u vezi s oblakom. U 2016. godini lansirala je Oracle Cloud Infrastructure (OCI, ranije Oracle Bare Metal Cloud Services). Oracle i dalje djeluje naslijeđenom uslugom, Oracle Cloud Infrastructure Classic, ali ona se ubrzano zastarjela u korist OCI-ja.

Ponuda: OCI nudi i VM-ove koji se plaćaju po satu, virtuelno prilagođene KVM-om, kao i poslužitelje Bare metal cloud services (uključujući instalaciju i konfiguraciju jednim klikom i Oracle Database, Real Application Clusters [RAC] i Exadata) i Docker usluga kontejnera sa sjedištem u Kubernetesu (Oracle Container Engine za Kubernetes). Oracle nudi i spremanje objekata (OCI Object Storage, ranije Oracle Bare Metal Cloud Object Storage). Oracle je prethodno Oracle Cloud ponudio kupcu, privatnu IaaS ponudu u oblaku, ali više se ne prodaje. Potrebe za kolokacijom zadovoljavaju se putem partnerske razmjene (Oracle FastConnect).

Lokacije: OCI centri podataka grupirani su u regije, od kojih neke imaju samo jednu zonu dostupnosti, poput one u Kanadi i Japanu. Regije s tri zone dostupnosti nalaze se na istoku i zapadu Sjedinjenih Država, a u Njemačkoj i Ujedinjenom Kraljevstvu Oracle ima globalnu prodaju. Dokumentacija portala OCI dostupna je samo na engleskom jeziku, ali portal je dostupan na 28 dodatnih jezika.

Preporučeni način rada: OCI će se svidjeti kupcima s uglavnom Oracleovim radnim opterećenjima s načinima rada 1 načina rada, posebno onima koji imaju performanse koji su dobro prilagođeni poslužiteljima golog metala i onima koji ne trebaju više od vrlo osnovnih mogućnosti IaaS u oblaku.

Preporučene uporabe: OCI je najprikladniji za poduzeća koja zahtijevaju oblak IaaS za Oracle aplikacije i za aplikacije za koje je potrebna Oracle baza podataka.

- **Prednosti**

Oracle-ova strategija oblaka usidrena je zbog njegovih aplikacija, baze podataka i drugog srednjeg softvera te obuhvaća IaaS, PaaS i SaaS. Oracleov oblak IaaS primarno je infrastrukturni temelj za ostale tvrtke. Oracle uglavnom cilja korisnike koji žele pokretati Oracle softver na cloud IaaS-u, posebno one koji se više vole baviti Exadata uređajima i poslužiteljima golog metala.

Nekoliko tvrtki Oracleovih loza uspjelo je dizajnirati istinsku hipersveliku arhitekturu. OCI se ističe po tome što je mogao privući vrhunske talente vodećih davatelja usluga oblaka kako bi ostvario cilj izgradnje dobro dizajnirane oblačne infrastrukture.
Oracle je tokom godina postigao dobar napredak u pogledu rasta novih kupaca i postojećih kupaca povećavajući upotrebu OCI. Referentni kupci također komentiraju pozitivne performanse platforme.

- **Mjere opreza**

Oracle na tržište vjerojatno neće ikada promatrati kao općenitog dobavljača integrirane ponude IaaS i PaaS. To je zbog dominacije pružatelja hiper-skale, Oracle-ov kasni početak s OCI-om i polarizirajuća priroda Oracle-a u glavama programera koji su često vodeći utjecaji na javni IaaS u oblaku.

Mnoge značajke razvijene za OCI neće OECI-jevu temeljnu korisničku bazu široko koristiti jer tvrtka gradi sposobnosti uglavnom kao odgovor na RFP-ove, koji su često dizajnirani prema mogućnostima etabliranih pružatelja hiper-skala.

U prošloj godini Oracle je prioritetno definirao svoj razvojni plan kao odgovor na povratne informacije kupaca. Primijenjena su osnovna obilježja upravljanja, na štetu značajnog kašnjenja uvođenja drugih usluga koje se smatraju trenutačno održivim na trenutnom oblaku IaaS u oblaku. Ovakav odmak od planiranih stavki mape puta treba očekivati, imajući u vidu prirodu OCI-ovih mogućnosti i potrebu dinamičkog prioriteta mape puta na temelju postignutih ponuda.

ALDI INICIJATIVA ZA INOVATIVNI TRENING

Panorama b.b. 73 000 Goražde

Bosna i Hercegovina

INTERNET OF THINGS

UMREŽAVANJE (NETWORKING)

AITI-IOT-001-180-03

Networking

Povezivanje svih stvari u Internet of Things

AITI

Skill Accelerator

Follow us at @UAITLab

Networking

Povezivanje svih stvari u Internet of Things

Početkom 20 stoljeća nafta je bila glavni motor do tada neviđenog progresa i napredka širom svijeta. Sto godina kasnije nafti se bliži kraj (kako zbog ograničenih resursa tako i zvog negativnog uticaja na okoliš) mjesto ključnog resursa na kojem se zasniva razvoj sve više preuzimaju podaci koji su glavni motor četvrte industrijske revolucija (Industrija 4.0).

U predhodnom poglavlju imali ste prilike kako bi napravili dobru strategiju. I kao što ste mogli primjetiti, korištenje ovih alata skoro pa bezvrijedno bez odgovarajućih, tačnih i relevantnih podataka.

Kako bi bili u mogućnosti da skoristite puni potencijal podataka u ovom poglavlju su obrađene teme koje će vam pomoći da usvojite znanja iz oblasti poslovnog obavještanja (Business Intelligence) čija primjena doprinosi boljem, bržem i efikasnijem donošenju odluka, te će steći vještine rada sa podacima u softverskim platformama za provođenje analitike podataka u poslovne svrhe.

U ovom poglavlju vi će te se moći upoznati sa:

- Osnovama pristupa poslovnog obavlještavanja i novim pristupima korištenja poslovnih podataka u procesu donošenja odluka u organizaciji;
- Osnovama rada sa podacima kako bi mogli iskoristiti njihov puni potencijal za primjenu poslovne analike u upravljačkim procesima;
- Mogućnostima koje nude softverkse platfome Tableau i Power BI, dvije trenutno najbolje softverske platforme za poslovnu analitiku i Business intelligence za mala i srednja preduzeća/organizacije.

Znanje sa kom se možete upoznati u ovom poglavlju sigurno će vam olakšati napore na razvoju vaših strateških ideja. Međutim, oni vam takođe mogu biti od izuzetne koristi kada budete razvijali vaše prijedloge projekata putem vi vaše strateške ideje razrađujete u detaljne planove akcije.

Poslovna analitika u doba podataka postaje sve važniji alat koji se primjenjuje u poslovanju, zato ne gubimo vrijeme i krenimo da se upoznamo sa ovom jako zanimljivom temom.

1. Mrežne tehnologije za IoT

Osnove mrežnih tehnologije za IoT; IoT mrežni protokoli

Osnove mrežne tehnologije za IoT

Mrežne tehnologije omogućavaju IoT uređajima da komuniciraju s drugim uređajima, aplikacijama i uslugama koje rade u Cloud-u. Internet se oslanja na standardizirane protokole kako bi se osigurala sigurna i pouzdana komunikacija između heterogenih uređaja. Standardni protokoli određuju pravila i formate koji uređaji koriste za uspostavljanje i upravljanje mrežama i prijenos podataka putem tih mreža.

Mreže su izgrađene kao "snop" (eng. Stack) tehnologija. Na dnu snopa nalazi se tehnologija poput Bluetooth LE. Dok su druge poput IPv6 tehnologije (koja je odgovorna za logično adresiranje uređaja i usmjeravanje mrežnog prometa) na vrhu snopa. Tehnologije na vrhu snopa koriste aplikacije koje se pokreću na tim slojevima, poput tehnologija čekanja poruka.

Za razvoj IoT projekta važno je da razuijete osnove mrežne tehnologije za IoT

Ova sekcija posvećena je upravo teme.

U njoj možete saznati osnove široko usvojenih tehnologija i standarda za IoT umrežavanje.

Takođe, ovde ćemo vam dati osnovne smjernice koje vam mogu pomoći da izvršite odabir odgovarajućeg mrežnog protokola za vaš projekat, te da razumijete ključna razmatranja i izazove povezane s umrežavanjem unutar IoT-a:

- domet,
- propusnost,
- potrošnja energije,
- povremena povezanost,
- interoperabilnost, i
- sigurnost.

Mrežni standardi i tehnologije

Model otvorenih sustava međusobnog povezivanja (eng. Open System Interconnection - OSI) je apstraktni ISO standard, a sastoji se od sedam slojeva protokola.

Gledajući odozgo prema dole OSI nivoi protokola su:

- aplikacija,
- prezentacija,
- sesija,
- transport,
- mreža,
- podatkovna veza, i
- fizička.

TCP / IP ili paket internetskih protokola podupire internet i pruža pojednostavljenu konkretnu implementaciju ovih slojeva u OSI modelu.

Prikaz. Modeli umrežavanja OSI i TCP / IP

OSI model	TCP/IP model
7 Application	Application
6 Presentation	
5 Session	
4 Transport	Transport
3 Network	Internet
2 Data link	Network access & physical
1 Physical	

TCP / IP model uključuje samo četiri sloja, spajajući neke od slojeva OSI modela:

- **Pristup mreži i fizički sloj**

Ovaj TCP / IP sloj obuhvaća oba OSI sloja 1 i 2. Fizički (PHY) sloj (Layer 1 OSI) upravlja kako je svaki uređaj fizički povezan s mrežom hardverom, na primjer optičkim kablom, žicama ili radiom u u slučaju bežične mreže poput wifi IEEE 802.11 a / b / g / n). Na sloju veze (Layer 2 OSI) uređaji se identificiraju prema MAC adresi, a protokoli na ovoj razini

bave se fizičkim adresanjem, poput načina na koji prekidači isporučuju okvire uređajima na mreži.

- **Internetski sloj**

Ovaj sloj preslikava na OSI Layer 3 (mrežni sloj). OSI 3. Layer odnosi se na logičko adresiranje. Protokoli na ovom sloju definiraju kako usmjerivači isporučuju pakete podataka između izvornih i odredišnih hostova identificiranih IP adresama. Za adresiranje IoT uređaja obično se prihvaća IPv6.

- **Transportni sloj**

Transportni sloj (Layer 4 u OSI) fokusiran je na komunikaciju od početka do kraja i pruža značajke poput pouzdanosti, izbjegavanja zagušenja i jamči da će se paketi isporučiti istim redoslijedom kojim su poslani. UDP (User Datagram Protocol) često se usvaja za IoT transport iz razloga performansi.

- **Sloj aplikacije**

Aplikacijski sloj (OSI Layer 5, 6 i 7) pokriva razmjenu poruka na razini aplikacije. HTTP/S je primjer protokola aplikacijskog sloja koji se široko prihvaća na internetu.

Iako vam TCP / IP i OSI modeli pružaju korisne apstrakcije za raspravu o mrežnim protokolima i specifičnim tehnologijama koje implementiraju svaki protokol, neki se protokoli ne uklapaju uredno u ove slojevite modele i nepraktični su.

Na primjer, sigurnosni protokol transportnog sloja (TLS) koji implementira šifriranje radi osiguranja privatnosti i integriteta podataka mrežnog prometa može se smatrati da djeluje na OSI slojevima 4, 5 i 6.

IoT mrežni protokoli

Neki od mrežnih protokola koji su široko usvojeni unutar IoT-a i koji se uklapaju u TCP / IP slojeve prikazani su na narednoj slici.

Mnogo novih i konkurentskih mrežnih tehnologija se usvajaju unutar IoT prostora. Višestruke tehnologije različitih dobavljača ciljaju različita vertikalna tržišta - automatizaciju kuća, zdravstvo ili industrijski IoT - i nude alternativne implementacije istih standardnih protokola. Na primjer, IEEE 802.15.4 opisuje rad bežičnih bežičnih osobnih mreža male brzine (LR-WPAN) i provodi ih nekoliko konkurentskih tehnologija, uključujući ZigBee, Z-Wave, EnOcean, SNAP i 6LoWPAN.

Prikaz: Protokoli IoT mreže preslikani na TCP / IP model

TCP/IP model	IoT protocols
Application	HTTPS, XMPP, CoAP, MQTT, AMQP
Transport	UDP, TCP
Internet	Ipv6, 6LoWPAN, RPL
Network access & physical	IEEE 802.15.4 Wifi (802.11 a/b/g/n) Ethernet (802.3) GSM, CDMA, LTE

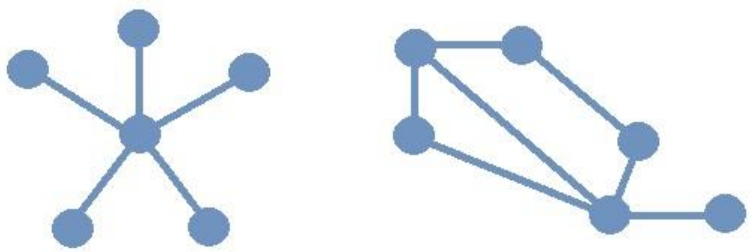
U IoT se mogu primijeniti tehnologije koje se koriste za internetsko povezivanje, poput Etherneta. Dok gledate dalje niz dionica prema fizičkim prijenosnim tehnologijama, suočavate se s više izazova koji su specifični za IoT uređaje i IoT kontekst.

Struktura mreže poznata je kao njena topologija. Najčešći mrežni topologiji koji su usvojeni unutar IoT-a su topologije zvijezda i mash.

U zvjezdanoj topologiji, svaki je IoT uređaj izravno povezan sa središnjim središtem (gatewayom) koji komunicira s podacima sa povezanih uređaja uzvodno.

U mash topologijama uređaji se povezuju s drugim uređajima unutar dosega. Čvorovi unutar mreže mogu djelovati kao jednostavni senzorski čvorovi. Senzorski čvorovi usmjeravaju promet kao i čvorovi gatewaya. Mash mreže su složenije od mreža sa zvjezdanim topologijama. Manje su skloni kvaru jer se ne oslanjaju na niti jedan središnji ulaz.

Prikaz: Star (Lijevo) i Mash (Desno) mrežne topologije



IoT mrežne tehnologije i pristup internetu na fizičkom sloju

IoT mrežne tehnologije kojih se treba znati na dnu snopa protokola uključuju mobilni, wifi i Ethernet, kao i specijalizirana rješenja kao što su LPWAN, Bluetooth Low Energy (BLE), ZigBee, NFC i RFID.

Gartner je pokazao da NB-IoT postaje standard za LPWAN mreže. O ovom standardu će biti više riječi malo kasnije.

Slijede mrežne tehnologije sa kratkim opisima svake:

1. LPWAN

Mreža široke mreže široke potrošnje (eng. Low Power Wide Area Network) kategorija je tehnologija dizajniranih za dugotrajnu bežičnu komunikaciju male snage. Idealni su za velike implementacije IoT uređaja male snage kao što su bežični senzori. LPWAN tehnologije uključuju LoRa (protokol fizičkog sloja LongRange), Haystack, SigFox, LTE-M i NB-IoT (Narrow-Band IoT).

2. Celularna

Standardi LPWAN NB-IoT i LTE-M bave se niskim, niskobudžetnim IoT komunikacijskim opcijama koristeći postojeće mobilne mreže. NB-IoT najnoviji je od ovih standarda i usredotočen je na dugoročnu komunikaciju između velikog broja primarno zatvorenih uređaja. LTE-M i NB-IoT razvijeni su posebno za IoT, međutim postojeće stanične tehnologije često su prihvaćene za bežičnu komunikaciju dugog dometa. Iako je ovo uključilo 2G (GSM) u naslijeđene uređaje (i trenutno se postupno ukida), CDMA (također u odlasku u mirovinu ili u postupnoj fazi ukidanja), ona također uključuje 3G koji se brzo ukida s nekoliko mrežnih pružatelja usluga koji povlače sve 3G uređaje. 4G je i dalje aktivan i bit će sve dok 5G ne postane u potpunosti dostupan i implementiran.

3. Bluetooth niska energija (BLE)

BLE je inačica popularnog protokola bežične komunikacije Bluetooth 2,4 GHz.

Dizajniran je za komunikaciju kratkog dometa (ne više od 100 metara), obično u zvjezdanoj konfiguraciji, s jednim primarnim uređajem koji kontrolira nekoliko sekundarnih uređaja.

Bluetooth djeluje na oba sloja 1 (PHY) i 2 (MAC) OSI modela. BLE je najprikladniji za uređaje koji u nizu prenose male količine podataka. Uređaji su dizajnirani tako da spavaju i štede energiju kada ne prenose podatke. Lični IoT uređaji, poput nosivih narukvica za zdravlje i fitness, često koriste BLE.

4. ZigBee

ZigBee djeluje na bežičnom komunikacijskom spektru 2,4 GHz. Ima duži domet od BLE do 100 metara. Ima i nešto nižu brzinu prijenosa (maksimalna 250 kbps u usporedbi s 270 kbps za BLE) od BLE.

ZigBee je Mesh mrežni protokol. Za razliku od BLE-a, ne mogu svi uređaji spavati između emitovanja. Mnogo ovisi o njihovom položaju u mreži i o tome trebaju li djelovati kao usmjerivači ili kontroleri unutar Mesh-a. ZigBee je dizajniran za izgradnju i automatizaciju kućnih aplikacija.

Još jedna usko povezana tehnologija ZigBee je Z-Wave, koji se također temelji na IEEE 802.15.4. Z-Wave dizajniran je za kućnu automatizaciju. To je vlasnička tehnologija, ali nedavno je objavljena kao specifikacija za javne domene.

5. NFC

Protokol komunikacije u blizini polja (eng. Near Field Communication NFC) koristi se za komunikaciju vrlo malog dometa (do 4 cm), poput držanja NFC kartice ili oznake pored čitača. NFC se često koristi za platne sisteme, ali je također koristan za sisteme za prijavu i pametne oznake u praćenju imovine.

6. RFID

RFID označava radiofrekvencijsku identifikaciju.

RFID oznake pohranjuju identifikatore i podatke. Oznake su pričvršćene na uređaje i čita ih RFID čitač. Tipični raspon RFID je manji od metra. RFID oznake mogu biti aktivne, pasivne ili pasivno potpomognute. Pasivne oznake idealne su za uređaje bez baterija, jer ih čitatelj pasivno čita. Aktivne oznake povremeno emitiraju svoj ID, dok potpomognute pasivne oznake postaju aktivne kada je prisutan RFID čitač. „Dash7“ je komunikacijski protokol koji koristi aktivni RFID koji je osmišljen za upotrebu u industrijskim IoT aplikacijama za sigurnu komunikaciju na duge udaljenosti. Slično kao u NFC-u, i tipični slučaj upotrebe RFID-a prati praćenje predmeta u maloprodajnim i industrijskim IoT aplikacijama.

7. Wi-Fi

Wifi je standardno bežično umrežavanje na temelju specifikacija IEEE 802.11a / b / g / n. 802.11n nudi najveći protok podataka, ali po cijenu velike potrošnje energije, pa bi IoT uređaji mogli koristiti samo 802.11b ili g samo iz razloga uštede energije.

Iako je wifi usvojen unutar mnogih prototipskih i trenutnih generacija IoT uređaja, kako rješenja daljnjeg i nižeg napajanja postaju široko dostupna, vjerojatno je da će wifi zamijeniti alternative s manjom snagom.

8. Ethernet

Ethernet implementira IEEE 802.3 standard široko razvijene za žično povezivanje u lokalnim mrežama. Međutim, vjerovatno je da vam neće trebati da vam svi IoT uređaji budu stacionarni i bežićno povezani.

Na primjer, senzorske jedinice instalirane unutar sustava automatizacije zgrada mogu koristiti tehnologije žičnog umrežavanja poput Etherneta. Alternativna kabelska mreža (PLC), alternativno rješenje s žičanom vezom, koristi postojeće električne ožičenje umjesto namjenskih mrežnih kablova.

Dolazak 5G mreža

5G je sljedeća generacija bežičnih mreža. Ona predstavlja nadogradnju postojeće 4G Long-Term Evolution (LTE) infrastrukture. Kod 5G značajno je poboljšana propusnost. Ali isto tako i kapacitet, te pouzdanost bežične usluge.

5G je idealan za više podataka i komunikacijskih zahtjeva koje postavljaju milijuni povezanih uređaja koji čine IoT. Njegova posebna osobina jeste vrlo nisko krajnje kašnjenje u komunikaciji u stvarnom vremenu (eng. ultra-low latency). To je potpuno novi cjevovod za podatke koji služi kao vodovod za svaki signal, iz svakog uređaja, koji koristi Internet. Njegova je prednost i to što može propuštati i velike/guste količine podataka.

Brz je - dvadesetak puta brži od 4G, što omogućava korisniku da preuzme trominutni UHD video, recimo, u samo 17 sekundi. To je poticaj za naš povezani svijet u doba IoT-a i vidljiv poticaj onome što IoT može postići u budućnosti.

Dolazak i potpuna primjena 5G još je u ranoj primjeni. Budite sigurni, učinit će naš svijet boljim, naše živote boljim i omogućiti plodovima tehnologije da sjaje tad više sjaj nego ikad prije dok se podaci kreću u većim količinama, brže nego ikad prije.

Internetski sloj IoT mrežne tehnologije

Tehnologije internetskog sloja (OSI Layer 3) identificiraju i usmjeravaju pakete podataka. Tehnologije koje se obično usvajaju za IoT povezane su s ovim slojem i uključuju IPv6, 6LoWPAN i RPL.

Upoznajmo se sada sa svakim od njih.

1. IPv6

Na internetskom sloju uređaji se identificiraju putem IP adresa. IPv6 se obično koristi za IoT aplikacije nad naslijeđenim IPv4 adresiranjem. IPv4 je ograničen na 32-bitne adrese, koje ukupno pružaju samo oko 4,3 milijarde adresa, što je manje od trenutnog broja

povezanih IoT uređaja, dok IPv6 koristi 128 bita i tako pruža 2*128 adresa (oko 3,4 × 10*38 ili 340 milijardi milijardi milijardi) adresa.

U praksi, ne trebaju svi IoT uređaji javne adrese.

Od desetaka milijardi uređaja za koje se očekuje da će se povezati putem IoT-a tokom sljedećih nekoliko godina, mnogi će biti raspoređeni u privatnim mrežama koje koriste raspon privatnih adresa i komuniciraju samo s drugim uređajima ili uslugama na vanjskim mrežama pomoću pristupnika.

2. 6LoWPAN

Standard IPv6 bežične osobne mreže male snage (IPv6 Low Power Wireless Personal Area network - 6LoWPAN) omogućava da se IPv6 koristi u 802.15.4 bežičnim mrežama. 6LoWPAN se često koristi za bežične senzorske mreže, a Thread protokol za uređaje za kućnu automatizaciju također radi preko 6LoWPAN.

3. RPL

Internetski sloj također pokriva usmjeravanje.

Protokol usmjeravanja IPv6 za mreže male snage i gubitke (RPL) dizajniran je za usmjeravanje IPv6 prometa preko mreža male snage poput onih koje se provode preko 6LoWPAN. RPL (izgovara se "ripple") dizajniran je za usmjeravanje paketa unutar ograničenih mreža, poput bežičnih senzorskih mreža, gdje nisu svi uređaji dostupni u svakom trenutku i postoje velike ili nepredvidive količine gubitka paketa. RPL može izračunati optimalni put izgradnjom grafa čvorova u mreži na temelju dinamičkih metrika i ograničenja poput minimiziranja potrošnje ili latencije energije.

Aplikacijski sloj IoT mrežnih tehnologija

HTTP i HTTPS su sveprisutni u internetskim aplikacijama, što vrijedi i unutar IoT-a, s RESTful HTTP i HTTPS okvirima.

CoAP (Protokol ograničene aplikacije) je lagan HTTP koji se često koristi u kombinaciji sa 6LoWPAN preko UDP-a.

Protokoli za razmjenu poruka poput MQTT, AMQP i XMPP često se koriste i u IoT aplikacijama:

1. MQTT

Telemetry Transport Message Querya (MQTT) je protokol za razmjenu poruka utemeljen na objavljivanju i pretplati, dizajniran za upotrebu u situacijama male propusnosti, posebno za senzore i mobilne uređaje u nepouzdanim mrežama.

2. AMQP

Napredni protokol čekanja poruka (AMQP) otvoreni je standardni protokol poruka koji se koristi za srednji softver orijentiran na poruke. Najvažnije je da AMQP implementira RabbitMQ.

3. XMPP

Proširivi protokol poruka i prisutnosti (XMPP) početno je dizajniran za komunikaciju između čovjeka i čovjeka u stvarnom vremenu, uključujući trenutne poruke.

Ovaj je protokol prilagođen za komunikaciju stroj-stroj (M2M) radi primjene laganog srednjeg softvera i usmjeravanja XML podataka. XMPP se prvenstveno koristi kod pametnih uređaja.

Vaš izbor tehnologija na ovom sloju ovisit će o specifičnim aplikativnim zahtjevima vašeg IoT projekta. Na primjer, za jeftiniji sistem za automatizaciju kućanstava koji uključuje nekoliko senzora, MQTT bi bio dobar izbor, jer je izvrstan za implementaciju poruka na uređajima bez puno pohrambene ili procesorske snage jer je protokol jednostavan i lagan za implementaciju.

MQTT protokol

Prije nego što je Internet of Things bio stvar, ili zapravo otprilike u vrijeme kada se pojam Internet of Things prvi put spominje u tisku (krajem 90-ih), surađivao sam s Arlenom Nipperom (danas iz CirrusLinka) na osmišljavanju protokola za komunikaciju sa SCADA-om sustavi u naftnoj i plinskoj industriji. Ono što je započelo kao visoko nišni protokol za određenu industriju, brzo je postalo broj jedan otvoreni kod za bilo koju komunikaciju IoT uređaja.

MQTT, model za razmjenu poruka s objavljivanjem i pretplatom

MQTT je protokol za razmjenu poruka, izgrađen na vrhu TCP / IP-a, koji se temelji na modelu razmjene poruka objaviti-pretplatiti. Izdavači šalju poruke, pretplatnici primaju poruke koje ih zanimaju, a brokeri poruke izdavača prenose pretplatnicima. Izdavači i pretplatnici su MQTT klijenti koji komuniciraju samo s MQTT posrednikom. MQTT klijenti mogu biti bilo koji uređaji ili aplikacije (od mikrokontrolera poput Arduina do cjelovitog poslužitelja aplikacija hostiranog u oblaku) koji pokreće MQTT knjižnicu i koji se povezuje s MQTT posrednikom preko mreže. MQTT brokeri upravljaju primanjem poruka od izdavača i slanjem poruka pretplatnicima (kao i upravljanjem popisima tema koje pretplatnike zanimaju).

MQTT kao Open source

Kako je Internet stvari odmicao, tako je odmicao i MQTT. Prvi MQTT broker s otvorenim kodom, Mosquitto, stvoren je 2008. godine, koji je 2014. postao projekt Eclipse Mosquitto. U 2012. godini projekt Eclipse Paho pružio je knjižnice klijenta MQTT s otvorenim kodom za Java, C, JavaScript i Python, a od tada je popis knjižnica klijenta MQTT rastao. Krajem 2014. godine, MQTT verzija 3.1.1 postaje OASIS standard, što je otvorilo put 2016. MQTT-u da postane ISO standard.

MQTT preuzima IoT

MQTT je vodeći protokol za povezivanje IoT uređaja, pretjecanje HTTP-a, oslonca na području Interneta, 2017. Štoviše, MQTT je odabran kao protokol za razmjenu poruka IoT platformi za Amazon, Microsoft i (naravno) IBM, kao kao i mnogi proizvodi otvorenog koda i drugi komercijalni brokeri. IBM-ova platforma Watson IoT pruža ne samo masovnu sigurnu povezanost za MQTT uređaje, već i upravljanje uređajima, pohranu podataka i analitiku podataka u IBM Cloudu. MQTT je također podnio test skalabilnosti postavši protokol za razmjenu poruka koji stoji iza Facebook Messengera.

Što je sljedeće za MQTT

Prvih deset godina njegovog života nismo napravili nikakve promjene u protokolu MQTT, što sugerira da smo prilično dobro predvidjeli potrebe tržišta i njegovih korisnika. Kako je Internet sazrijevao, zajedno s industrijskim uređajima i povezivanjem, te pojavom velikog hostinga u oblaku, shvatili smo da MQTT trebaju neke dodatne značajke. Bilo mi je važno da ostanemo vjerni "temeljnim načelima" MQTT-a: uglavnom da je to kompaktna, lako razumljiva i jednostavna za implementaciju specifikacija. MQTT v5 objavljen je krajem 2018. godine, a na putu je da bude ratificiran kao OASIS, a potom ISO, početkom 2019. godine. U međuvremenu, svakodnevno stotine milijuna uređaja i aplikacija šalju i primaju podatke i naredbe putem Interneta stvari, koristeći MQTT.

Rad sa MQTT protokolom

Za IoT uređaje povezivanje s Internetom svojevrsni je uvjet. Povezivanje s Internetom omogućuje uređajima međusobnu suradnju i pozadinske usluge. Temeljni mrežni protokol Interneta je TCP / IP. Izgrađen na vrhu TCP / IP stoga, MQTT (Message Queue Telemetry Transport) postao je standard za IoT komunikaciju. MQTT se također može izvoditi na SSL / TLS-u, što je sigurni protokol izgrađen na TCP / IP-u, kako bi se osiguralo da je sva podatkovna komunikacija između uređaja šifrirana i sigurna.

MQTT je izvorno izumio i razvio IBM krajem 1990-ih. Njegova prvotna primjena bila je povezivanje senzora na naftovodima sa satelitima. Kao što mu samo ime govori, to je protokol za razmjenu poruka koji podržava asinkronu komunikaciju između strana. Asinhroni protokol za poruke razdvaja pošiljatelja i primatelja poruka i u prostoru i u vremenu te je stoga prilagodljiv u nepouzdanim mrežnim okruženjima.

Što je MQTT i zašto bih ga trebao koristiti?

MQTT je lagan i fleksibilan mrežni protokol koji postiže pravu ravnotežu za IoT programere:

- Lagani protokol omogućuje njegovu primjenu na strogo ograničenom hardveru uređaja, kao i na mrežama velike kašnjenja / ograničene propusnosti.
- Njegova fleksibilnost omogućuje podršku različitim scenarijima aplikacija za IoT uređaje i usluge.

Da bismo razumjeli zašto je MQTT tako pogodan za IoT programere, prvo ispitajmo zašto drugi popularni mrežni protokoli nisu uspjeli u IoT-u.

Zašto je MQTT bolji od drugih protokola

Većina programera već su upoznati s HTTP web uslugama. Pa, zašto se IoT uređaji jednostavno ne povežu s web uslugama? Uređaj je mogao slati svoje podatke kao HTTP zahtjev i primati ažuriranja iz sustava kao HTTP odgovor. Ovaj obrazac zahtjeva i odgovora ima neka ozbiljna ograničenja:

- HTTP je sinkroni protokol. Klijent čeka da poslužitelj odgovori. To je uvjet za web preglednike, ali dolazi po cijenu loše skalabilnosti. U svijetu IoT-a velik broj uređaja i najvjerojatnije nepouzdana mreža / mreža velikih kašnjenja čine sinkronu komunikaciju problematičnom. Protokol asinkrone razmjene poruka puno je prikladniji za IoT aplikacije. Senzori mogu poslati očitanja i omogućiti mreži da utvrdi optimalan put i vrijeme za isporuku do odredišnih uređaja i usluga.
- HTTP je jednosmjeran. Klijent mora inicirati vezu. U IoT aplikaciji uređaji ili senzori su obično klijenti, što znači da ne mogu pasivno primati naredbe s mreže.
- HTTP je protokol 1-1. Klijent daje zahtjev, a poslužitelj odgovara. Teško je i skupo emitirati poruku na sve uređaje na mreži, što je čest slučaj u IoT aplikacijama.
- HTTP je protokol velike težine s mnogo zaglavlja i pravila. Nije prikladno za ograničene mreže.

Iz gore navedenih razloga, većina skalabilnih sustava visokih performansi koristi internu sabirnicu za razmjenu poruka, umjesto internetskih usluga, za internu razmjenu podataka. U stvari, najpopularniji protokol za razmjenu poruka koji se koristi u sustavima internetskog softvera za poduzeće naziva se AMQP (Advanced Message Queuing Protocol). Međutim, u okruženju visokih performansi računarska snaga i kašnjenje mreže obično nisu problem. AMQP je dizajniran za pouzdanost i interoperabilnost u poslovnim aplikacijama. Ima bogat set značajki, ali nije prikladan za IoT ograničene resurse.

Osim AMQP-a, postoje i drugi popularni protokoli za razmjenu poruka. Na primjer, XMPP (Extensible Messaging and Presence Protocol) je protokol razmjene neposrednih poruka (IM). Teška je za značajke koje podržavaju slučajeve korištenja IM-a, poput prisutnosti i medijskih privitaka. U usporedbi s MQTT-om, zahtijeva mnogo više resursa kako na uređaju tako i na mreži.

Pa, što MQTT čini tako laganim i fleksibilnim? Ključna značajka MQTT protokola je njegov model objavljivanja i pretplate. Kao i kod svih protokola za razmjenu poruka, on razdvaja izdavača i potrošača podataka.

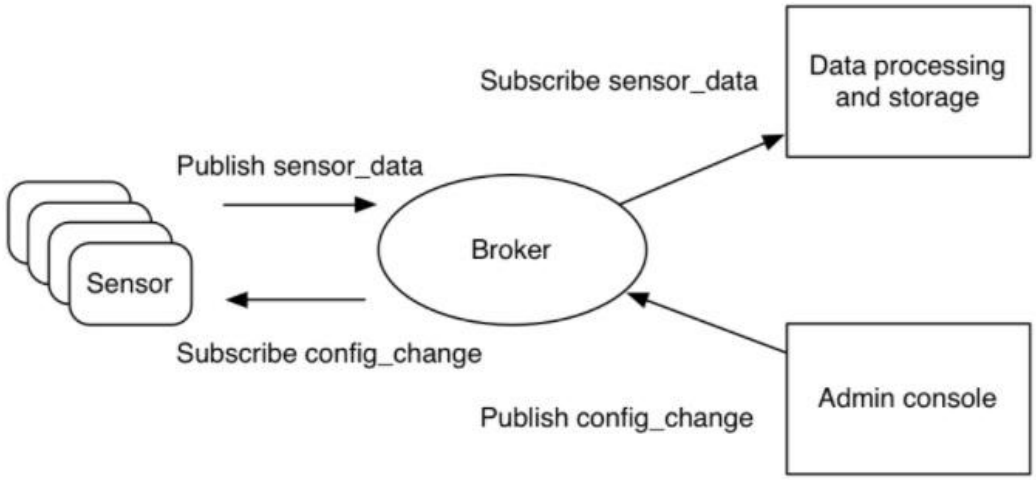
Model objavljivanja i pretplate

MQTT protokol definira dvije vrste entiteta u mreži: posrednik poruka i broj klijenata. Posrednik je poslužitelj koji prima sve poruke od klijenata, a zatim te poruke usmjerava na relevantne odredišne klijente. Klijent je sve što može stupiti u interakciju s posrednikom za slanje i primanje poruka. Klijent može biti IoT senzor na terenu ili aplikacija u podatkovnom centru koji obrađuje IoT podatke.

1. Klijent se povezuje s posrednikom. Može se pretplatiti na bilo koju poruku "teme" u posredniku. Ova veza može biti obična TCP / IP veza ili šifrirana TLS veza za osjetljive poruke.
2. Klijent objavljuje poruke pod temom slanjem poruke i teme posredniku.
3. Posrednik zatim prosljeđuje poruku svim klijentima koji su pretplaćeni na tu temu.

Budući da su MQTT poruke organizirane po temama, programer aplikacija ima fleksibilnost da odredi da određeni klijenti mogu komunicirati samo s određenim porukama. Na primjer, senzori će objaviti svoja očitanja pod temom "data_data" i pretplatiti se na temu "config_change". Aplikacije za obradu podataka koje spremaju podatke senzora u pozadinsku bazu podataka pretplatit će se na temu "data_senzor". Aplikacija administratorske konzole mogla bi primati naredbe administratora sustava za podešavanje konfiguracija senzora, poput osjetljivosti i učestalosti uzorka, i objaviti te promjene u temi "config_change".

Prikaz: MQTT model publikovanja i predplate za IoT senzore



Početak rada s razvojem MQTT-a

Najlakši alat za započinjanje s razvojem MQTT-a je modul mosquitto, koji je dio projekta Eclipse koji pruža MQTT SDK-ove i knjižnice na više programskih jezika. Sadrži posrednika MQTT koji se može pokretati na vašem lokalnom računalu i alatima naredbenog retka za interakciju s posrednikom pomoću poruka.

Modul možete preuzeti i instalirati s web mjesta komaraca. Obavezno instalirajte i mosquitto (posrednik) i mosquitto_clients (klijenti) module.

Naredba install na Ubuntu Linux je sljedeća.

```
$ sudo apt-get install mosquitto mosquitto-clients
```

Naredba za instaliranje na RedHat Linux je sljedeća.

$ sudo yum -y install epel-release $ sudo yum -y install mosquitto

Naredba mosquitto pokreće posrednika MQTT na vašem lokalnom računalu. Po želji biste mogli koristiti opciju -d da biste je pokrenuli u pozadini.

```
$ mosquitto -d
```

Možete ga pokrenuti i kao sistemsku uslugu.

```
$ systemctl start mosquitto
```

Dalje, u drugom prozoru terminala možete upotrijebiti naredbu mosquitto_sub za povezivanje s lokalnim posrednikom i pretplatu na temu. Jednom kada se naredba izvrši, pričekat će i ispisati svaku poruku koju primi putem pretplate čim dođu.

```
$ mosquitto_sub -t "dw/demo"
```

U još jednom prozoru terminala možete upotrijebiti naredbu mosquitto_pub za povezivanje s lokalnim posrednikom, a zatim objaviti poruku na temu.

```
$ mosquitto_pub -t "dw/demo" -m "hello world!"
```

Sada bi terminal koji pokreće mosquitto_sub sada trebao ispisati pozdrav svijetu! na ekranu. Upravo ste poslali i primili poruku putem MQTT brokera!

Za više opcija o tome kako koristiti alate za komarce, kao i o tome kako koristiti mosquitto API za stvaranje vlastitih MQTT klijentskih aplikacija, pogledajte njegovu dokumentaciju

Korištenje IBM-ove platforme Internet of Things kao posrednika MQTT-a

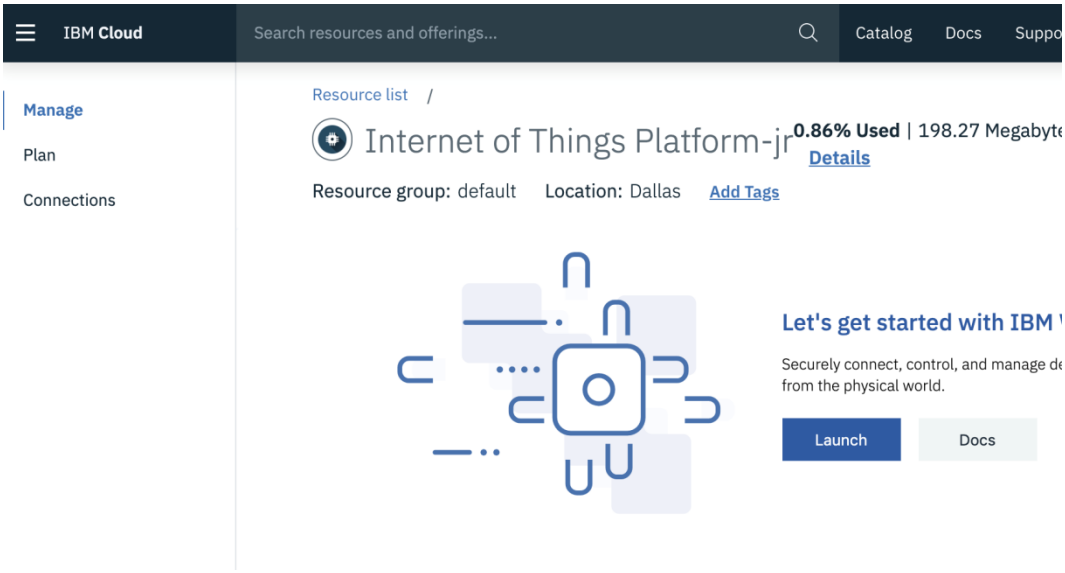
Naravno, u proizvodnom sistemu ne možete koristiti lokalno računalo kao posrednika. IBM Internet of Things (IoT) platforma pruža pouzdanu uslugu na zahtjev koja funkcionira poput MQTT posrednika. Usluga IBM IoT Platform poboljšava standardnog posrednika MQTT na nekoliko različitih načina: pruža predmemoriju posljednjeg događaja; omogućuje konfiguraciju trajnosti podataka; podržava protokole za upravljanje uređajima; i pruža analitičke mogućnosti.

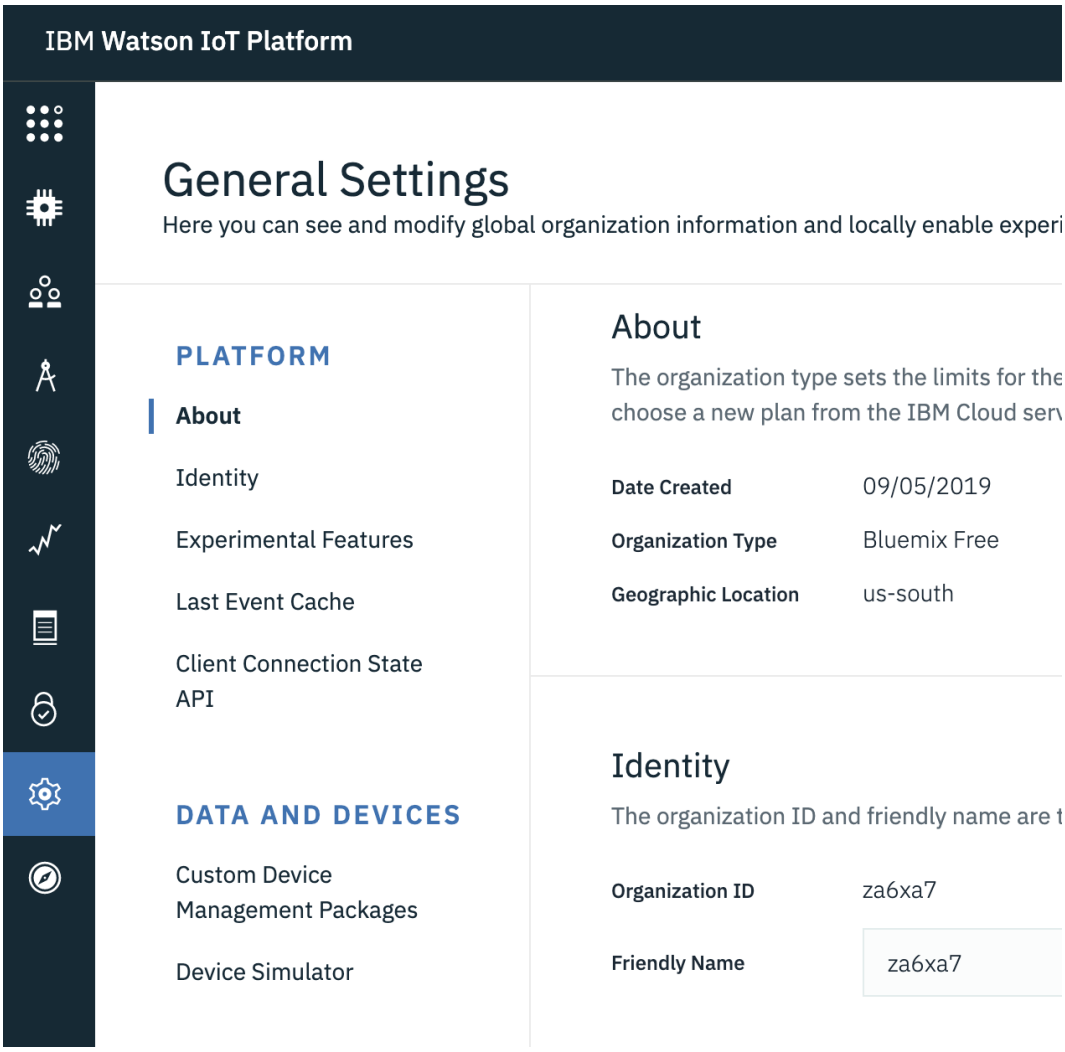
Na IBM Cloud konzoli kliknite „**Catalog“**, „**Internet of Things“**, a zatim odaberite „**Internet of Things Platform“**. Odatle možete odabrati plan usluge. Lite plan je besplatan i pruža dovoljno mogućnosti za većinu malih projekata.

Jednom kada stvorite instancu usluge IoT platforme, možete kliknuti dugme "**Launch**" u odjeljku "upravljanje" da biste je pokrenuli.

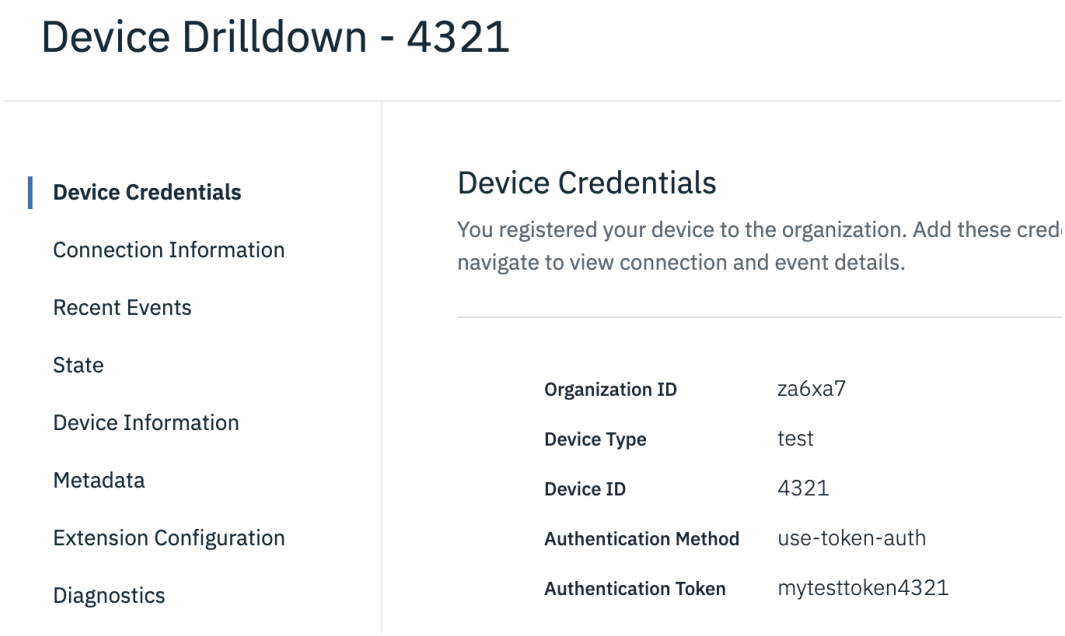
Zabilježite “ID organizacije” instance vaše platforme na zaslonu. ID organizacije nalazi se i u URL-u upravljačke konzole:

Prikaz: Konfigurisanje MQTT na IBM IoT Platformi

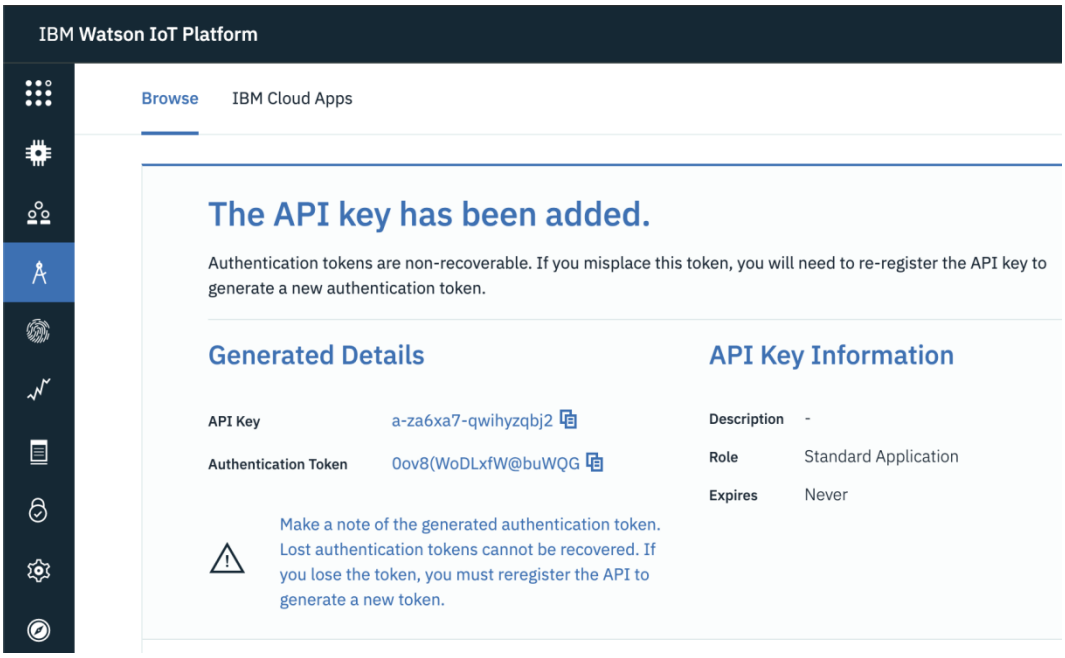




Dalje, u odjeljku Uređaji možete stvoriti novi uređaj. Uređaj ima vrstu i ID. Ovdje izrađujemo uređaj tipa ispitivanja i 4321 ID.



Napokon, možete stvoriti dvije aplikacije za slanje poruka u ime uređaja i za primanje poruka s uređaja na obradu. Svaka aplikacija ima ID i pristupni token.



Prije nego što smo se mogli koristiti naredbama mosquitto za povezivanje s posrednikom MQTT na IBM IoT platformi, potrebne su nam sljedeće postavke povezivanja.

Domaćin MQTT brokera je za6xa7.messaging.internetofthings.ibmcloud.com. Primijetite da je za6xa7 ID organizacije za instancu usluge.

Trebat će vam datoteka certifikata da biste pokrenuli sigurnu TLS vezu s posrednikom. TLS je za IBM IoT Platform zadan prema zadanim postavkama, jer bi vjerodajnice za pristup trebale biti šifrirane preko mreže. Sadržaj datoteke messaging.pem nalazi se ovdje:https://github.com/ibm-watson-iot/iot-python/blob/master/src/wiotp/sdk/messaging.pem

Sada se pomoću sljedećeg naredbenog retka pretplatite na statusne događaje za uređaj koji smo upravo stvorili iz jedne od naših aplikacija. Primijetite da koristi TLS šifrirani kanal na portu 8883 i vjeruje certifikatu poslužitelja u messaging.pem.

```
$ mosquitto_sub -t "iot-2/type/test/id/4321/evt/status/fmt/+" -h za6xa7.messaging.internetofthings.ibmcloud.com -p 8883 --cafile messaging.pem -u a-za6xa7-bwrus5qab4 -P auth-token-here -i a:za6xa7:test2
```

Zatim upotrijebite sljedeću naredbu za slanje JSON poruke na događaj uređaja iz druge aplikacije.

```
$ mosquitto_pub -t "iot-2/type/test/id/4321/evt/status/fmt/json" -m "{\"mesg\" : \"hello IBM\"}" -h za6xa7.messaging.internetofthings.ibmcloud.com -p 8883 --cafile messaging.pem -u a-za6xa7-lxmzussonj -P auth-token-here -i a:za6xa7:test1
```

Gornji naredbeni prozor mosquitto_sub trebao bi sada ispisati poruku na konzolu.

Sad kad imate nužne alate, zaronimo dublje u MQTT protokol.

Savjeti i zaobilaznice

Snaga MQTT-a je njegova jednostavnost. Nemate ograničenja na vrste tema ili korisni teret poruka koje možete koristiti. To omogućuje neke zanimljive slučajeve upotrebe. Na primjer, razmotrite ova pitanja:

Kako mogu poslati 1-1 poruku s MQTT-om? Obje se strane mogu složiti da će koristiti temu koja je jedinstvena za njih. Na primjer, naziv teme mogao bi sadržavati ID-ove oba klijenta kako bi se osigurala njegova jedinstvenost.

Kako klijent emitira svoj status prisutnosti? Sustav bi mogao imati dogovorenu konvenciju imenovanja za teme "prisutnosti". Na primjer, tema "prisutnost / id klijenta" može sadržavati podatke o prisutnosti za klijenta. Klijent postavlja poruku na istinito kad se poveže i na lažno kad se prekida. Klijent također može postaviti zadnju poruku volje na false, tako da se postavlja kada veza prekida. Posrednik može zadržati poruku kako bi novi klijenti mogli pročitati temu i saznati status prisutnosti.

Kako mogu osigurati komunikaciju? Veza klijent-posrednik može biti šifrirana TLS veza za zaštitu podataka u prijenosu. Uz to, budući da MQTT protokol ne nameće ograničenja na format podataka o korisnom opterećenju, sustav bi mogao imati dogovorenu metodu šifriranja i mehanizam za ažuriranje ključa. Nakon toga, sav sadržaj korisnog tereta mogao bi biti šifrirani binarni podaci stvarnih JSON ili XML poruka.

Izazovi IoT umrežavanja

Kada razmislite koje mrežne tehnologije usvojite u vašoj IoT aplikaciji, imajte na umu slijedeća ograničenja:

- Opseg
- Širina pojasa
- Potrošnja energije
- Isprekidano povezivanje
- interoperabilnost
- Sigurnost

Opseg

Mreže se mogu opisati udaljenostima preko kojih podaci obično prenose IoT uređaji priključeni na mrežu:

- **PAN (Personal Area Network)**

PAN je kratkog dometa, gdje se udaljenosti mogu mjeriti u metrima, kao što je nosivi uređaj za praćenje fitnessa koji komunicira s aplikacijom na mobitelu preko BLE.

- **LAN (Local Area Network)**

LAN je kratkog do srednjeg dometa, gdje udaljenost može biti i do stotina metara, poput kućne automatizacije ili senzora koji su instalirani unutar tvorničke proizvodne linije koji komuniciraju preko wifija s pristupnim uređajem instaliranim unutar iste zgrade.

- **MAN (Metropolitan Area Network)**

MAN je dugog dometa (područje grada), gdje se udaljenosti mjere i do nekoliko kilometara, poput pametnih parking senzora instaliranih u gradu, koji su povezani u mrežnu topologiju mreže.

- **WAN (Wide Area Networka)**

WAN je dugotrajni, na kojem se udaljenosti mogu mjeriti u kilometrima, poput poljoprivrednih senzora koji su instalirani na velikoj farmi ili ranču koji se koriste za nadgledanje okolišnih mikroklima.

Mreža bi trebala dohvatiti podatke s IoT uređaja i prenijeti ih na predviđeno odredište. Odaberite mrežni protokol koji odgovara rasponu. Na primjer, nemojte odabrati BLE za WAN aplikaciju koja će raditi na udaljenosti od nekoliko kilometara. Ako prijenos podataka u potrebnom rasponu predstavlja izazov, razmislite o rubnom računarstvu. Ručno računanje analizira podatke izravno s uređaja, a ne iz udaljenog podatkovnog centra ili negdje drugdje.

Širina pojasa

Širina propusnosti je količina podataka koja se može prenijeti u jedinici vremena. Ograničava brzinu kojom se podaci mogu prikupljati s IoT uređaja i prenositi uzvodno. Na širinu pojasa utječu mnogi faktori, koji uključuju:

- Količina podataka koji svaki uređaj prikuplja i prenosi
- Broj raspoređenih uređaja
- Bilo da se podaci šalju kao konstantan tok ili s povremenim rafalima i jesu li značajna razdoblja vrha

Veličina paketa mrežnog protokola treba odgovarati količini podataka koja se obično prenosi. Neefikasno je slati pakete podstavljene praznim podacima. Suprotno tome, postoje dijelovi za dijeljenje većih dijelova podataka na previše malih paketa. Brzine prijenosa podataka nisu uvijek simetrične (to jest, brzine prijenosa mogu biti sporije od brzina prijenosa). Ako postoji dvosmjerna komunikacija između uređaja, prijenos podataka mora se uzeti u obzir. Bežične i mobilne mreže su tradicionalno male propusne širine, pa razmislite je li bežična tehnologija pravi izbor za aplikacije velikih količina podataka.

Razmislite trebaju li se prenijeti svi neobrađeni podaci. Moguće rješenje je prikupiti manje podataka rijeđim uzorkovanjem. Tako ćete snimiti manje varijabli i filtrirati podatke s uređaja možete ispustiti nevažne podatke. Ako podatke skupite prije nego što ih pošaljete, smanjujete volumen podataka. Ali ovaj postupak utječe na fleksibilnost i preciznost u analizi uzvodne prodaje. Agregiranje i raščlamba nisu uvijek pogodni za podatke koji su osjetljivi na vrijeme ili kašnjenje. Sve ove tehnike povećavaju zahtjeve za obradom i pohranom podataka za IoT uređaj.

Potrošnja energije

Prijenos podataka s uređaja troši energiju. Za prijenos podataka na velikim rasponima potrebno je više energije nego na kratkom rasponu. Morate uzeti u obzir izvor napajanja - poput baterije, solarne ćelije ili kondenzatora - uređaja i njegov ukupni životni ciklus. Dug i trajan životni ciklus ne samo da će pružiti veću pouzdanost, već će smanjiti troškove rada. Mogu se poduzeti koraci za postizanje duljih životnih ciklusa napajanja. Na primjer, kako biste produžili vijek trajanja baterije, uređaj možete prebaciti u stanje mirovanja kad god radi u praznom hodu. Druga najbolja praksa je modeliranje potrošnje energije uređaja pod različitim opterećenjima i različitim mrežnim uvjetima kako bi se osiguralo da se napajanje i kapacitet skladištenja uređaja podudaraju sa snagom koja je potrebna za prijenos potrebnih podataka pomoću mrežnih tehnologija koje ste usvojili.

Isprekidana povezanost

IoT uređaji nisu uvijek povezani. U nekim su slučajevima uređaji osmišljeni za povremeno povezivanje. Međutim, ponekad nepouzdana mreža može uzrokovati ispadanje uređaja zbog problema sa povezivanjem. Ponekad su problemi s kvalitetom usluge, poput rješavanja smetnji ili ometanja kanala na bežičnoj mreži koristeći zajednički spektar. Dizajni bi trebali uključivati isprekidanu povezanost i tražiti svaka dostupna rješenja za pružanje neprekidne usluge, ako bi to trebao biti kritični faktor za IoT krajolik dizajn.

interoperabilnost

Uređaji rade s drugim uređajima, opremom, sustavima i tehnologijom; interoperabilni su. S toliko različitih uređaja koji se povezuju s IoT-om interoperabilnost može biti izazov. Usvajanje standardnih protokola bio je tradicionalni pristup za održavanje interoperabilnosti na Internetu. Standarde dogovaraju sudionici u industriji i izbjegavaju više različitih dizajna i uputa. Uz odgovarajuće standarde, a sudionici koji se s njima

slažu, mogu se izbjeći problemi s nekompatibilnošću, stoga se mogu izbjeći problemi interoperabilnosti.

Međutim, za IoT se postupci standardizacije ponekad trude pratiti inovacije i promjene. Napisani su i objavljeni na temelju nadolazećih verzija standarda koje su još uvijek podložne promjenama. Razmotrimo ekosustav oko tehnologija: jesu li široko usvojeni? Jesu li otvoreni prema vlasničkim? Koliko je implementacija dostupno?

Pomoću ovih pitanja za planiranje vaših IoT mreža pomažete u planiranju bolje interoperabilnosti za robusniju IoT mrežu.

Sigurnosti

Sigurnost je prioritet. Izbor mrežnih tehnologija koje implementiraju zaštitu od kraja do kraja, uključujući provjeru autentičnosti, šifriranje i zaštitu otvorenih portova je presudan. IEEE 802.15.4 uključuje sigurnosni model koji pruža sigurnosne značajke koje uključuju kontrolu pristupa, integritet poruke, povjerljivost poruke i zaštitu od ponovnog ponavljanja, a implementirane su na tehnologijama koje se temelje na ovom standardu kao što je ZigBee.

Uzmite u obzir sljedeće čimbenike u oblikovanju sigurne i IoT mreže:

- **Autentikacija**

Usvojite sigurne protokole za podršku provjere autentičnosti za uređaje, pristupnike, korisnike, usluge i aplikacije. Razmislite o korištenju standarda X.509 za provjeru autentičnosti uređaja.

- **Enkripcija**

Ako koristite wifi, za šifriranje bežične mreže koristite bežični zaštićeni pristup 2 (WPA2). Također možete usvojiti pristup privatnom unaprijed podijeljenom ključu (PPSK). Da biste osigurali privatnost i integritet podataka za komunikaciju između aplikacija, obavezno usvojite TLS ili Datagram transportnu razinu zaštite (DTLS) koja se temelji na TLS-u, ali prilagođena za nepouzdane veze koje prelaze preko UDP-a. TLS šifrira podatke programa i osigurava njihov integritet.

- **Zaštita porta**

Zaštita porta osigurava da samo vanjski priključci potrebni za komunikaciju s pristupnikom ili upstream aplikacijama ili uslugama. Svi ostali priključci trebaju biti onemogućeni ili zaštićeni zaštitnim zidovima. Priključci uređaja mogu biti izloženi pri korištenju Universal Plug and Play (UPnP) ranjivosti. Stoga bi UPnP trebao biti onemogućen na usmjerivaču.

2. Tehnologije niske snage za razmjene podataka na širokom području (LPWAN)

Osnove LPWAN tehnologija; NB-IoT; LoRa tehnologije; Sigfox; Wi-Fi HaLow; Celularne mreže (GPRS / 3G / 4G / 5G)

Pravilan odabir IoT mreža umrežavanja zahtijeva kompromise. Odabrane mrežne tehnologije utjecati će na dizajn IoT uređaja. Razmatranja predložena u ovoj sekciji zavise o mnogim faktorima.

Na primjer, mrežni raspon, brzina prijenosa podataka i potrošnja energije izravno su povezani. Ako povećate mrežni raspon ili brzinu i volumen podataka koji se prenose, vašim IoT uređajima će sigurno trebati dodatna snaga za prijenos podataka u tim uvjetima.

Za osnovnu automatizaciju kuće, kriterij razmatranja snage vjerojatno je malo važan; uređaj će se najvjerojatnije napajati izravno iz zidne utičnice. Ograničenja propusne širine i odustajanja od povezivanja veći su prioriteti. Wifi pruža razumnu propusnost i ubrzava projekt korištenjem robnog hardvera. Međutim, wifi nije optimiziran za uređaje male potrošnje, što ga čini nepromišljenim izborom za uređaje sa baterijom.

Ovo do sada vam govori da je za vas važno da odmah na početku razumijete neke od najčešćih mrežnih protokola i tehnologija umrežavanje IoT.

Zapamtite da je najvažnije je razmotriti svoje zahtjeve u svjetlu IoT mrežnih izazova kako biste pronašli tehnologije koje će najbolje odgovarati vašoj IoT aplikaciji.

Upoznajmo se sada sa nekim od IoT tehnologija umrežavanja koje mogu poslužiti vašem novom projektu.

Osnove LPWAN tehnologija

Povećavanjem mogućnosti za pretvaranje običnih stvari u „pametne“ prilikom dizajniranja novog IoT projekta sučit će te se sa potrebom za korištenjem uređaja koji će biti u mogućnosti da sa malom snagom/potrošnjom energije na velike udaljenosti prenose male količine podataka. Do sada su za ovu potrebu uglavnom bile korištene 3G / 4G tehnologije koji nisu optimizirani za tu svrhu.

Sada vam tehnologija široke mreže male snage (LPWAN) stoji kao idealna opcija.

Trenutno na tržištu postoje različite LPWAN tehnologije, čiji odabir bi trebali da temeljite na osnovu svojih potreba.

LPWAN je stekao popularnost posljednjih godina, a očekuje se da će se taj trend ubrazno nastaviti u budućnosti. Za uređaje male snage koji prenose male podatke na velike udaljenosti, LPWAN nudi mogućnost koja djeluje efikasnije od ostalih bežičnih tehnologija. "Mnoge potencijalno povezane stvari" nalaze se u udaljenim ili teško dostupnim područjima na velikim udaljenostima od sljedeće stanične bazne stanice.

LPWAN je jako korisan kada imate slabu pokrivenost, kada je loša i kada vaš uređaj zahtijeva da radi sa velikom snagom da bi se povezao na mrežu.

Pored toga, mobilne mreže nisu optimizirane za aplikacije koje prenose samo male količine rijetkih podataka. Nadalje, postojeći stanični standardi ne podržavaju mogućnosti uštede energije, što ove standarde čini neprikladnim za jeftine uređaje kojima je potrebno nekoliko godina trajanja baterije.

Bežični prijenos s krajnjih čvorova IoT često mora komunicirati na velikim udaljenostima ili treba probiti barijere poput betona ili tla. LPWAN tehnologije su dobra opcija za ove uslove, omogućujući podacima koji mogu biti nepristupačni ili preskupi za pristup da bi bili povezani s Cloud-om

LPWAN veze pomažu pružiti više uvida u ono što se događa u fizičkom svijetu - to jest putem senzorskih čvorova u našim kućama, uredima, tvornicama i urbanoj infrastrukturi - pridonoseći tako analitikama temeljenim na oblaku u stvarnom vremenu."

Trenutno postoje mnoge LPWAN tehnologije; tu se ubrajaju NB-IoT, LoRa, Sigfox, HaLow, RPPM i Weightless. Svaka od njih ima jedinstvene značajke i karakteristike koje bi korisnici trebali znati prije nego što odluče koja tehnologija je za njih najprikladnija.

Saznajmo sada malo više o njima.

NB-IoT

Uskopojasni IoT (eng. Narrowband IoT – NB-IoT) je tehnološko rješenje koje je proizašlo iz potrebe za povezivanje velikog broja IoT uređaja bežičnom mrežom na velikoj udaljenosti.

S milijardama uređaja koje će se u bliskoj budućnosti pojaviti na mreži, trebat će nam bežične mreže koje ih mogu podržati. Je li Narrowband IoT (NB-IoT) rješenje?

Prema posljednjim istraživanjima sa kraja 2019. godine trenutno je aktivno 7,6 milijardi IoT uređaja, a očekuje se da će taj broj porasti na 24,1 milijardu do 2030.

Uz tako ogroman broj uređaja koji dolaze putem interneta trebat će nam siguran i pouzdana mreža da ih sve podrži. Velike nade u zadovoljavanje ove potrebe za povezivanjem IoT uređaja usmjerene su ka NB-IoT.

Da bi bili sigurni da je NB-IoT prava opcija tehnologije povezivanja za vaš projekat u ovoj sekciji ćemo pokušati objasniti kako funkcionira NB-IoT i pomoći vam da utvrdite je li to ispravna opcija povezivanja za vašu IoT implementaciju.

Što je Narrowband IoT?

Usko pojasni IoT (poznat i kao NB-IoT ili LTE-M2) je tehnologija LPWAN koja ne funkcionira u licenciranom LTE konstruktu. Umjesto toga, djeluje na jedan od tri načina:

- Nezavisno
- U neiskorištenim opsezima od 200 kHz koji su prethodno korišteni za GSM (Globalni sustav za mobilne komunikacije)
- Na LTE baznim stanicma koje dodjeljuju resursni blok operacijama NB-IoT ili u svojim zaštitnim opsezima.

Telekomunikacijski divovi kao što su Huawei, Ericsson, Qualcomm i Vodafone zajedno su ovaj standard zajedno s 3GPP-om.

Huawei, Ericsson i Qualcomm zainteresirani su za NB-IoT jer ima niz prednosti.

Uvođenje NB-IoT na licenciranom spektru znači poboljšanu pouzdanost za korisnike kao i zagarantovanu raspodjelu resursa potrebnih za upravljani QoS.

Prednosti poslovanja

Nekoliko je ključnih prednosti koje NB-IoT može donijeti vašem projektu. To su:

1. Energetska efikasnost

Efikasno napajanje IoT uređaja je presudno. Razmislite o tome: tko želi biti vani i mijenjati baterije na 20 milijardi uređaja svakih šest mjeseci? Iako su gotovo sve IoT tehnologije razvijene za štednju energije kada ne rade, oni troše energiju kada modem radi i rukuje s obradom signala.

2. Ušteda troškova

Tehnologije jednostavnijeg valnog oblika - poput NB-IoT - trošit će manje energije.

NB-IoT frontend i digitalizator 200 kHz nudi smanjenu složenost analogno-digitalne (A / D) i digitalno-analogne (D / A) konverzije, buferovanja i ocjene kanala.

To dovodi do slijedećeg: ušteda energije = ušteda troškova.

Uz to, NB-IoT čipove je jednostavnije stvoriti i na taj način ih jeftinije dobiti.

3. Pouzdanost

Uvođenje NB-IoT na licenciranom spektru znači poboljšanu pouzdanost korisnika kao i zajamčenu raspodjelu resursa koja je potrebna za upravljanje kvalitetom usluge (eng. Quality of Service - QoS).

4. Široka primjena

U usporedbi s LTE-M1, NB-IoT ima niže brzine prijenosa i niže troškove povezivanja. Uz to, prema Huaweijevom Emmanuel Coehlo Alvesu u članku o IoT Hub-u, NB-IoT ne trebaju pristupnici za omogućavanje povezivanja.

Umjesto da "stvorite još jedan dio opreme potreban za upravljanje i rukovanje", rekao je, NB-IoT može izravno povezati senzore s baznom stanicom. To će povećati fleksibilnost uz smanjenje troškova.

5. Globalni doseg

Iako su velike kompanije u SAD-u već uložili milijarde u LTE mreže, u mnogim je zemljama širom svijeta manje LTE-a, iako su piloti i umrežavanje mreža u punom zamahu. Izvan Sjedinjenih Država postoje veće razmještaje GSM na kojima možete pronaći neiskorištene opsege koje bi utjecale na NB-IoT. NB-IoT bi tada mogao pomoći IoT inovatorima da pronađu pristupačne ulazne točke na novim tržištima u svijetu.

Čak i u SAD-u, manji prijevoznici kao što su Sprint ili T-Mobile također mogu primijeniti NB-IoT na postojećem GSM spektru kako bi proširili povezanost bez LTE ulaganja Verizon ili AT&T.

Nadamo se da će se i u Bosni i Hercegovini napraviti pomak na ovom polju. Posebno zato jer je hrvatski telekom još prije dvije godine predstavio NB-IoT tehnologiju.

NB-IoT aplikacije

NB-IoT ima razne aplikacije od pametnog parkiranja do pametnih hotela. „Ova tehnologija je veoma prikladna za upotrebu u hotelima. Ovo će rješenje stvoriti vrijednost za hotele i za goste kao da će moći dodati digitalne ključeve aplikacijama za vjernost hotela. Ona može pojednostaviti poslovanje hotela i pomoći im da prikupe podatke kako bi poboljšali cjelokupno iskustvo gostiju.

NB-IoT ima veliki potencijal za primjenu u područjima koja ne trebaju struju na licu mjesta ili Wi-Fi, poput ormarića za dostavu paketa, spremišta, brave ormara, pa čak i vozila.

NB-IoT aplikacije mogu prijeći mnoge kategorije usluga. To uključuje:

- Pametno mjerenje (struja, plin i voda)
- Usluge upravljanja objektima
- Protuprovalni i požarni alarmi za kuće i poslovne prostore
- Priključeni osobni uređaji koji mjere zdravstvene parametre
- Praćenje osoba, životinja ili predmeta
- Infrastruktura pametnih gradova poput uličnih svjetiljki ili kanti za otpatke
- Priključeni industrijski uređaji, poput aparata za zavarivanje ili kompresora za zrak.

Potencijalne barijere

S NB-IoT raspoređenim u bočnom pojasu, mogli bi se povećati početni troškovi na razvoju operativnog softvera. Nadalje, modemske linije i antene mogu postati složenije u slučajevima kada je malo GSM spektra. Konačno, postoji rizik da bi divovi ISP-a mogli povećati troškove licenciranja.

Ipak, s toliko nedovoljno iskorištenog 200-kHz GSM spektra mnogi žele učiniti ovo najboljom širokom mrežom niske snage dosad. Stoga nije čudo što Gartner NB-IoT vidi kao ključni dio LPWAN krajolika. A s početkom 5G, stanični IoT ima još svjetliju budućnost.

LoRa tehnologije

LoRa (skraćeno od eng. Long Range) je protokol široke mreže male snage (LPWAN) koji je razvila kompanija Semtech. Zasniva se na tehnikama modulacije širenja spektra proizašlih iz Chirp Spread Spectrum (CSS) tehnologije.

Semtechovi LoRa uređaji i tehnologija bežične radiofrekvencije dugačka je bežična platforma male snage koja je postala de facto tehnologija za IoT mreže širom svijeta. LoRa uređaji i otvoreni LoRaWAN® protokol omogućuju pametne IoT aplikacije koje rješavaju neke od najvećih izazova s kojima se suočava naš planet: upravljanje energijom, smanjenje prirodnih resursa, kontrola zagađenja, efikasnost infrastrukture, sprečavanje katastrofa i još mnogo toga. Semtechovi LoRa uređaji i LoRaWAN protokol skupili su nekoliko stotina poznatih slučajeva upotrebe pametnih gradova, pametnih kuća i zgrada, pametne poljoprivrede, pametnog mjerenja, pametnog lanca opskrbe i logistike i još mnogo toga. Sa više od 100 milijuna uređaja povezanih s mrežama u 100 zemalja i raste, LoRa uređaji stvaraju pametniju planetu.

LoRa bežična RF tehnologija

Semtech inovacija, LoRa uređaji nude upečatljive karakteristike za IoT aplikacije, uključujući duge domete, malu potrošnju energije i siguran prijenos podataka.

Tehnologija se može koristiti javnim, privatnim ili hibridnim mrežama i pruža veći raspon od celulrne mreže. LoRa tehnologija lako se može priključiti na postojeću infrastrukturu i omogućava niskobudžetne IoT aplikacije na baterije.

Semtechovi LoRa čipseti Semtech ugrađeni su u uređaje proizvedene od strane velikog ekosistema dobavljača rješenja IoT i povezani s LoRaWAN mrežama širom svijeta. Jednostavno rečeno, LoRa povezuje uređaje (ili sve stvari) s Cloudom.

Otvorena specifikacija LoRaWAN je protokol nisko napajanja širokog područja (LPWAN) koji se temelji na LoRa tehnologiji. Dizajniran za bežično povezivanje stvari koje koriste baterije na Internetu u regionalnim, nacionalnim ili globalnim mrežama, LoRaWAN protokol koristi nelicencirani radio spektar u opsegu Industrial, Science and Medical (ISM). Specifikacija definira uređaj do infrastrukture LoRa parametara fizičkog sloja i LoRaWAN protokol i pruža besprijekornu interoperabilnost između uređaja. Dok Semtech pruža LoRa radio čipove, LoRa Alliance®, neprofitna asocijacija i najbrže rastući tehnološki savez, pokreće standardizaciju i globalno usklađivanje LoRaWAN protokola.

LoRaWAN je popularna LPWAN tehnologija. LoRa Alliance uključuje prestižne IT kompanije, uključujući Cisco, IBM i Renesas.

LoRaWAN odašilje podatke brzinom od 0,3 kbps do 50 kbps. Uređaji razmjenjuju podatke na 200 kHz opsegu za razmjenu radio poruka putem zraka, pri čemu je svaka poruka široka 100 Hz i prenosi se sa 100 ili 600 bita u sekundi, ovisno o regiji.

LoRa protokol je najprikladniji za aplikacije gradskog nadzora. „To uključuje različite raširene krajnje čvorove koji se često nalaze u teško dostupnim okruženjima. Dobar primjer je senzor vibracije ugrađen u most, koji pruža podatke o fizičkom stanju mosta i potencijalnom kvaru uzrokovanom stresom.

Primjena LoRaWAN tehnologije

LoRa tehnologija najviše cilja M2M.

Aplikacije za LoRa bežičnu tehnologiju uključuju pametno mjerenje, praćenje zaliha, podatke o prodajnim strojevima i nadzor, automobilsku industriju i komunalne aplikacije.

Te su tehnologije široko implementirane i integrirane u mnogim sisitema, čak i mala računala poput Arduinoa imaju LoRa mogućnosti. U skladu s tim, vrlo je lako razvijati LoRa aplikacije za proizvodnju velikih razmjera ili za više specijalnih aplikacija.

LoRa tehnologija revolucionirala je IoT omogućujući prijenos podataka u velikom rasponu, a pritom koristi vrlo malo energije. Kad su spojeni na necelularnu LoRaWAN mrežu, LoRa uređaji prihvaćaju širok raspon IoT aplikacija odašiljući pakete s važnim informacijama. LoRaWAN

popunjava tehnološki jaz mobilnih i Wi-Fi / BLE mreža temeljenih na mrežama koje zahtijevaju ili veliku propusnost ili veliku snagu, ili imaju ograničen domet ili nemogućnost prodiranja u duboka unutarnja okruženja. Zapravo,

LoRa tehnologija je fleksibilna za slučajeve ruralne ili zatvorene upotrebe u pametnim gradovima, pametnim kućama i zgradama, pametnoj poljoprivredi, pametnom mjerenju i pametnom lancu nabave i logistike.

Sigfox

Sigfox su osnovali Ludovic Le Moan i Christophe Fourtet 2010. godine s vizijom da svaki objekt u našem fizičkom svijetu povežu s digitalnim svemirom. Dvojica francuskih osnivača izgradila su globalnu mrežu posvećenu Internetu stvari na temelju male snage, dugog dometa i malih podataka koji nudi uslugu povezivanja s kraja na kraj. Od samog početka Sigfox pokreće održiv i povezan svijet, uvodeći novu internetsku revoluciju.

U samo nekoliko godina Ludovic Le Moan prikupio je gotovo 300 milijuna eura od strateških i financijskih investitora u Europi, Sjedinjenim Državama i Aziji kako bi podržao širenje globalne mreže 0G. 0G mreža je low-cost - low power bežična mreža dizanirana da salje i prima kratke poruke između IoT uređaja. Osnovao je i „IoT Valley“, prvi europski IoT ekosistem koji je pomogao startapima da ubrzaju usvajanje interneta stvari.

Sada prisutan u više od 70 zemalja, Sigfox je prvi igrač koji je izgradio najveći IoT ekosistem na svijetu, od velikih proizvođača do stotina startupa i proizvođača uređaja na četiri kontinenta.

Sigfox tehnologija

Sigfox uvodi prvu globalnu mrežu 0G za povezivanje milijardi objekata koji emitiraju podatke, bez potrebe za uspostavljanjem i održavanjem mrežnih veza.

Ovaj jedinstveni pristup u svijetu bežične povezanosti, gdje nema nadzemnih signalizacija, kompaktan i optimiziran protokol i gdje udio predmeta nije povezan s mrežom.

Mreža 0G je jeftina bežična mreža male snage namijenjena slanju ili primanju malih poruka između IoT uređaja. Sigfox je inicijator mreže 0G. Da bi to učinili, stvorili su vlastitu mrežnu tehnologiju koja je sada dostupna u 65 zemalja i omogućuje objektima da neovisno i sigurno komuniciraju.

Mreža 0G omogućava IoT uređajima da se povezuju s njegovom mrežom putem interneta i prenose male količine podataka u velikim rasponima. Ova jeftina mreža ne zahtijeva skupe IoT uređaje sa SIM karticama.

Mreža 0G vrlo je sigurna i manje podložna mrežnim napadima jer omogućuje samo jednosmjernu komunikaciju između uređaja i bazne stanice. Nakon razmjene informacija, uređaj prelazi u stanje mirovanja, što daje vrlo mali prozor kako bi hakeri provalili u mrežu i preuzeli kontrolu.

Ova je mreža također imuna na napade distribuiranog uskraćivanja usluge (DDoS) u kojima je mreža preplavljena s toliko poruka da se isključuje. Prijenos podataka 0G mreže slučajne je prirode, što onemogućava zastoj.

Mreža Sigfox 0G idealna je za IoT, Industry 4.0 aplikacije, uključujući lanac opskrbe i logistiku, pametne gradove i pametne zgrade.

Sigfox nudi softversko komunikacijsko rješenje temeljeno na složenosti mreže i cloud Computing, a ne na uređajima. Sve to zajedno drastično smanjuje potrošnju energije i troškove povezanih uređaja.

Wi-Fi HaLow

Wi-Fi HaLow razvio je Wi-Fi Alliance. Ova tehnologija djeluje u 900 MHz radijskom spektru (za razliku od 2,4 GHz i 5 GHz za tradicionalni Wi-Fi) i zasnovana je na prenosu podataka u širokom rasponu od 150 kilobita u sekundi do 18 megabita u sekundi.

Glavna prednos WiFi HaLow tehnologije u odnosu na tradicionalnu wifi mrežu je u tome što ima opseg transmisije do do jednog kilometra.

Postavljanje HaLow mreže u osnovi je isto što i postavljanje Wi-Fi-ja. Senzor integriran s HaLow tehnologijom, primjerice u obliku HaLow modula, povezan je s Wi-Fi pristupnom točkom. Podaci se prenose u pristupnu točku, a zatim se šire na Internet. Prednost Wi-Fi HaLow za primjenu u IoT je u tome što može da koristi ogromnu instaliranu bazu Wi-Fi uređaja.

Wi-Fi HaLow prikladan je za unutarnju i vanjsku primjenu, posebno u zahtjevnim RF okruženjima gdje su zidovi, beton i druge prepreke. Zbog ovoga je ova tehnologija sjajna prilika za korištenjem na mjestima kao što su podzemne garaže Senzori na svakom parkirnom mjestu mogu se povezati putem Wi-Fi HaLow na glavnu mrežu, a ljudi sa pametnim telefonima mogu vidjeti koja su parkirna mjesta otvorena, a koja zauzeta.

Karakteristike i prednosti WiFi HaLow za IoT

Osnovne karakteristike ove tehnologije su rad na spektru manjem od 1 GHz, pri čemu koristi uski band OFDM kanala, da posjeduje nekoliko načina rada za štednju energije, da ima native IP podršku i da osigurava visok nivo sigurnosti podataka.

Osnovne prednosti Wi-Fi HaLow za IoT su:

- Veliki domet (približno 1 km)
- Prolazak signala kroz zidove i druge barijere
- Može koristiti baterije tipa metalne novčanice za rad mjesecima ili godinama
- Nema potrebe za instaliranjem habova ili getveja.

Kao dio Wi-Fi portfolia, Wi-Fi HaLow omogućuje cjelovitiji pristup bežičnom povezivanju. Wi-Fi HaLow može pružiti mnoge pogodnosti koje danas potrošači očekuju od Wi-Fi-ja, uključujući interoperabilnost mnogih dobavljača, jednostavno postavljanje bez narušavanja postojeće Wi-Fi mreže i najnoviju sigurnost Wi-Fi-ja.

Wi-Fi HaLow nudi jedinstveni, otvoreni, industrijski standard koji može adresirati mnoge IoT aplikacije u više industrija. Kombinira doseg, robusnost, skalabilnost i energetsku efikasnost koju zahtijevaju IoT sistemi, s dodatnim prednostima i mogućnostima Wi-Fi-ja.

Rad u frekvencijskom spektru ispod 1 GHz i korištenje užih kanala omogućuje Wi-Fi HaLow pružanje do 100 puta dužeg raspona od ostalih opcija IoT tehnologije.

Može prodirati kroz građevinske materijale, osiguravajući uspješne instalacije za automatizaciju kuća i građevina bez skupih mreža ili repetitora, te povezivati uređaje udaljene otprilike jedan kilometar ili više, dok su druge IoT tehnologije dizajnirane tako da dosegnu samo 10 metara.

Wi-Fi HaLow koristi nekoliko metoda za postizanje veće energetske učinkovitosti od većine postojećih WAN mreža male snage i bežičnih PAN tehnologija. Koristeći nova poboljšanja MAC-a i načine mirovanja, Wi-Fi HaLow podržava uređaje koje pokreću baterijske kovanice; Učinkovito može upravljati senzorskim mrežama u različitim okruženjima, s povećanim kapacitetom za podršku do 8.191 uređaja po SSID-u.

Wi-Fi HaLow olakšava cjelovitiji pristup bežičnom povezivanju. Budući da je Wi-Fi, lakše se integrira s postojećim Wi-Fi mrežama, podržava izvorno IP umrežavanje i pruža najnovije Wi-Fi sigurnost. Visoka propusnost podataka i arhitektura s malim kašnjenjem omogućuju IoT uređajima prijenos zaštićenih podataka na aplikacijskim poslužiteljima temeljenim na oblaku. Ako su nadogradnje na terenu neophodne, Wi-Fi HaLow pruža kapacitet za učinkovita, sigurna ažuriranja putem zraka, minimizirajući vrijeme trajanja uređaja. To se sve može učiniti bez potrebe za vlasničkim pristupnicima ili čvorištima koje koriste arhitekture koje nisu Wi-Fi mreže, a koje se obično koriste u drugim IoT sistemima.

Celularne mreže (GPRS / 3G / 4G / 5G)

Dobro uspostavljena na tržištu potrošačke mobilne mreže, mobilne mreže nude pouzdanu širokopojasnu komunikaciju koja podržava različite glasovne pozive i aplikacije za streaming videa. S druge strane, nameću vrlo visoke operativne troškove i zahtjeve za napajanjem.

Iako mobilne mreže nisu održive za većinu IoT aplikacija koje pokreću senzorske mreže na baterije, oni se dobro uklapaju u posebne slučajeve upotrebe kao što su povezani automobili ili vozni park u transportu i logistici. Na primjer, info-zabava u automobilu, usmjeravanje prometa, napredni sustavi pomoći vozaču (ADAS), zajedno s telematikom i uslugama praćenja voznog parka, mogu se pouzdati u sveprisutnu i široku propusnost mobilne mreže.

Stanični 5G sljedećeg roda s podrškom za brzu pokretljivost i ultra-niskim kašnjenjem pozicioniran je kao budućnost autonomnih vozila i proširene stvarnosti. Očekuje se da će 5G u stvarnom vremenu omogućiti video nadzor radi javne sigurnosti, mobilnu dostavu medicinskih podataka u stvarnom vremenu za povezano zdravlje i nekoliko vremenski osjetljivih aplikacija za industrijsku automatizaciju.

3. Tehnologije kratkog dometa za prenos podataka

Osnove mrežnih tehnologije za IoT; IoT mrežni protokoli

Wi-Fi

Wi-Fi praktički nema potrebe objašnjavati s obzirom na njegovu kritičnu ulogu u pružanju prijenosa podataka s visokim propusnostima i za poslovno i kućno okruženje. Međutim, u prostoru IoT-a, njegova velika ograničenja u pokrivenosti, skalabilnosti i potrošnji energije čine tehnologiju mnogo manje prevladavajućom.

Namećući velike potrebe za energijom, Wi-Fi često nije izvedivo rješenje za velike mreže IoT senzora koji rade na baterije, posebno u industrijskim scenarijima IoT i pametnim zgradama. Umjesto toga, to se više odnosi na povezivanje uređaja koji se mogu prikladno spojiti na utičnicu kao što su uređaji i uređaji pametne kuće, digitalne signalizacije ili sigurnosne kamere.

Wi-Fi 6 - najnovija Wi-Fi generacija - donosi znatno poboljšanu propusnost mreže (tj. <9,6 Gbps) radi poboljšanja protoka podataka po korisniku u zagušenim okruženjima. Ovim je standard postavljen na podizanje javne Wi-Fi infrastrukture i transformiranje korisničkog iskustva s novim digitalnim mobilnim uslugama u maloprodaji i masovnoj zabavi. Također, očekuje se da će interne mreže za zabavu i dijagnostiku u vozilu biti slučaj korištenja Wi-Fi 6. koji će se najviše mijenjati u igrama. Ipak, razvoj će vjerojatno potrajati još neko vrijeme.

Potpuno novi Wi-Fi 6.0, poznat i kao 802.11ax, obećava ne samo 30% do 40% brže brzine prijenosa podataka, već i bolju potrošnju energije i performanse u prenapučenim područjima u usporedbi s prethodnikom.

Uloga WiFi u IoT

Kako se Internet stvari (IoT) ubrzava, postat će daleko veća potražnja za vezama mašina-mašina (M2M), od kojih su mnoge bežične. To će dovesti do još veće raznolikosti zahtjeva za performanse, što će odražavati ogroman broj različitih slučajeva upotrebe koji se mogu pojaviti pod kapom IoT-a.

Niti jedna tehnologija neće odgovoriti na sve te zahtjeve, a kao što ste se već mogli upoznati, postoji dugačak popis bežičnih IoT protokola. To će se vjerojatno konsolidirati s vremenom, ali sigurno će postojati potreba za barem jednom otvorenom, standardiziranom tehnologijom za nekoliko ključnih IoT profila. Ti se profili razlikuju o stupnju u kojem podržavaju:

- Izuzetno niska i umjerena snaga
- Dugi i lokalni raspon prema vrlo kratkom
- Niska brzina umjerene brzine podataka
- Ultra niska latencija vs niska latencija
- Kritična raspoloživost prema standardnoj dostupnosti
- Nelicencirani i licencirani spektar

WiFi ima prednost u pokrivanju vrlo širokog raspona profila zbog širenja wifi porodice standarda. To znači da će igrati ulogu u većini IoT okruženja, samostalno ili surađujući s više specijaliziranih protokola samostalno ili u saradnji sa mobilnim (celularnim) mrežama. Nekim IoT aplikacijama, kao što su usluge automobila ili video-aplikacije poput povezanih sigurnosnih kamera, trebat će propusni opseg bežične širokopojasne mreže implementiran kako bi se omogućili drugi zahtjevi poput niskog kašnjenja (u kritičnim se okruženjima to može dogoditi u privatnoj mreži ili kriška).

WiFi je jedinstveno dizajniran za podršku širokopojasnih i uskopojasnih IoT aplikacija sa zajedničke platforme koja može raditi na različitim razinama potrošnje energije i raspona signala. Sljedeće izdanje standarda 5G (izdanje 16), dat će prioritet IoT usmjerenim mogućnostima, kao što su latencija ispod četiri milisekunde i vrlo velika dostupnost, kako bi se podržali novi slučajevi u kategoriji URLLC (ultra-pouzdana komunikacija male latencije).

IoT aplikacije imaju različite zahtjeve za povezivanje u smislu raspona, protoka podataka, energetske efikasnosti i troškova uređaja. WiFi je često očigledan izbor jer je pokrivenost WiFi ugrađivanjem gotovo sveprisutna, ali nije uvijek odgovarajući izbor.

Zahtjevi za prijenos podataka za IoT razlikuju se od malih, povremenih korisnih opterećenja poput komunalnih brojila do velikih količina kontinuiranih podataka, kao što su video nadzor u stvarnom vremenu. Zahtjevi za domet mogu se kretati od vrlo kratkih udaljenosti do nosivih materijala do nekoliko kilometara za primjenu vremena i poljoprivrede

Ono što je zajedničko je ograničenje moći. IoT uređaji zahtijevaju stalnu povezanost, ali ne moraju imati stalni pristup izvoru energije.

Prednosti i nedostaci korištenja WiFi u IoT

WiFi, ili 802.11, bežični je protokol izgrađen s namjerom da zamijeni Ethernet bežičnom komunikacijom preko nelicenciranih opsega. Njegov je cilj bio osigurati jednostavno korištenje, jednostavno implementirati, jednostavno koristiti bežično povezivanje

kratkog dometa s interoperabilnošću među dobavljačima. Uz nulte troškove, mali je fokus na spektralnu efikasnost i uz očekivanu upotrebu stolnih uređaja, energetska učinkovitost nije bila presudna.

WiFi je očit izbor za IoT povezivanje jer je unutarnja WiFi pokrivenost gotovo sveprisutna, no nije uvijek odgovarajući izbor.

Prikaz: Prednosti i nedostaci wifi

Za	Protiv
1. Niski troškovi infrastrukture i uređaja	1. Visoka potrošnja energije
2. Jednostavna instalacija	2. Umjereni doseg
3. Sveprisutnost	3. Zagušenje spektra

Standardni WiFi, iako je očit izbor za IoT, ima ograničenja i u rasponu i u energetskoj učinkovitosti. IEEE je riješio ove nedostatke objavljivanjem specifikacija za 802.11ah i 802.11ax:

- **WiFi HaLow (802.11ah):** WiFi HaLow tehnologija temelji se na IEEE802.11ah standardu ratificiranom u septembru 2016. godine. Uvedena je posebno za rješavanje problema i raspona IoT-a. 802.11ah koristi opseg 900 MHz ISM izuzetan od dozvole za pružanje proširenog raspona uz male zahtjeve za napajanjem. Potrošnja električne energije dodatno se optimizira korištenjem unaprijed definiranih razdoblja budnosti i odmora te omogućava doseg preko radijusa od jednog kilometra. Omogućuje grupiranje stanica da minimizira svađu i relej kako bi proširio domet.

  No 802.11ah zahtijevat će specijalizirane bežične pristupne točke (ili radio stanice unutar AP-ova) i hardver klijenta. Iako je protokol ratificiran u listopadu 2016., bilo je vrlo malo entuzijazma za WiFi HaLow od dobavljača čipova.

- **HEW (802.11ax).** Nadolazeći visokoefikasni bežični (IEEE802.11ax) standard također dodaje brojne značajke pogodne za IoT. Zadržava ciljano vrijeme buđenja i značajke grupiranja stanica od 802.11ah da bi klijentima bio energetski štedljiv i izbjegao sudare. Uz to, višekorisne MIMO mogućnosti uzlazne veze, zajedno s manjim razmakom (78.125 kHz) podnožjem, dopuštaju do 18 klijenata istovremeno slanje podataka unutar kanala od 40 MHz.

Usvajanje 802.11ax u IoT-u ovisit će o troškovima klijenata sa 802.11ax i tome koliko brzo klijenti i AP-ovi dolaze na tržište.

Ono što na kraju možemo reći za WiFi tehnologiju u IoT jeste da standardni WiFi (zasnovan na 802.11a / b / g / n / ac) često nije najbolja tehnologija za IoT, ali određene IoT aplikacije mogu iskoristiti instalirani standardni WiFi, posebno u zgradama ili u kampusu. Očiti slučajevi uključuju automatizaciju zgrada i kuća i upravljanje energijom u kući, gdje se instalirani WiFi može koristiti kao komunikacijski kanal, a uređaji mogu biti povezani s električnim utičnicama.

Bluetooth i BLE

Vjerujemo da su mnogi postali jako familijarni sa Bluetooth tehnologijom.

Prvenstveno zahvaljujući pametnim telefonima.

Definiran u kategoriji bežičnih osobnih mreža, Bluetooth je komunikacijska tehnologija kratkog dometa dobro postavljena na tržištu potrošača. Bluetooth Classic izvorno je bio namijenjen razmjeni podataka između uređaja potrošača od točke do tačke ili od tačke do više tačaka (do sedam podređenih čvorova).

Bluetooth Classic

Bluetooth je tehnološki standard za bežični prijenos podataka kratkog dometa između uređaja koji imaju kompatibilne čipove.

Ova je tehnologija dizajnirana tako da ponudi jeftinu alternativu za Wi-Fi s niskom cijenom i niskom snagom na štetu raspona prijenosa koji je znatno kraći i brzine prijenosa.

Uspjeh i širenje ovog standarda zaslužna je za grupu tvrtki koja se zove Bluetooth Special Interest Group (SIG), koja je bila zadužena za njegov razvoj.

Treba reći da upotreba izraza "klasični Bluetooth" nije ispravno. Iako je ovaj izraz postao uobičajena upotreba i odnosi se na osnovnu brzinu Bluetooth. Bluetooth je u početku dizajniran za aplikacije koje zahtijevaju stalnu razmjenu protoka podataka. To znači da možete razmijeniti puno podataka na bliskoj udaljenosti.

BLE

Optimiziran za potrošnju energije, Bluetooth Low-Energy (BLE) je novija tehnologija koja je dizajnirana za rješavanje malih potrošačkih IoT aplikacija.

Uređaji koji omogućuju BLE uglavnom se koriste zajedno s elektroničkim uređajima, obično pametnim telefonima koji služe kao središte za prijenos podataka u oblak. Danas je BLE široko integriran u fizičku i medicinsku opremu (npr. Pametne satove, mjerače glukoze, pulsne oksimetre itd.) Kao i uređaje Smart Home (npr. Brave na vratima) - pri čemu se podaci prikladno komuniciraju i vizualiziraju na pametnim telefonima.

Objavljivanje specifikacije Bluetooth Mesh u 2017. ima za cilj omogućiti veću razmjeru BLE uređaja, posebno u maloprodajnim okvirima. Pružajući svestrane značajke lokalizacije u zatvorenom prostoru, BLE mreže svjetala korištene su za otključavanje novih inovacija usluga poput navigacije u trgovini, prilagođenih promocija i isporuke sadržaja.

Povezivanje je ključni stub svakog IoT sistema. Najvažniji faktori odlučivanja za odabir pravih bežičnih protokola koji se koriste za aplikaciju uključuju brzinu, raspon prijenosa, sigurnost, kompatibilnost i potrošnju energije. Pokrili smo pregled različitih bežičnih tehnologija na početku ovog poglavlja. U ovom dijelu usredotočit ćemo se na Bluetooth nisku energiju (BLE) i istražiti ključne karakteristike koje čine tehnologiju izbora mnogim IoT dizajnerima.

Bluetooth je pronašao nišu u bežičnim uređajima za ljudsko sučelje i audio perifernim uređajima s vezama za PC i mobilni telefon, što je kataliziralo tržište. Iako je napredak u Wi-Fi uređajima male snage osigurao alternativno povezivanje za neke aplikacije, potražnja za Bluetoothom i dalje je velika. S druge strane, BLE se razvio u švicarsku vojsku s povezivanjem zbog svoje fleksibilnosti profila, jednostavnosti uporabe s mobilnim telefonima i karakteristika ultra-male snage. BLE zamjenjuje vlasničke protokole poput ZigBee-a kako bi postao de-facto standard povezivanja u niskobudžetnim IoT uređajima.

Taj rast potiču nedavna ažuriranja BLE 5.0 i BLE 5.1 koja su poboljšala BLE-ove specifikacije. Na primjer, poboljšani asortiman osigurava da se bilo koji BLE uređaj poput pametnog senzora, pametne brave ili žarulje može besprijekorno povezati s bilo kojeg mjesta u kući. Ovo je ključni korak ka omogućavanju istinske pamene kuće. Poboljšani raspon također ima koristi kao što su pametni satovi tako da mogu primati trenutne obavijesti sa pametnih telefona koji se nalaze u drugoj sobi.

Još jedno značajno poboljšanje je značajno povećanje brzine prijenosa podataka, čineći prijenos podataka bogatijim i pametnijim. Usluge bez veze, poput svjetionika koji pružaju kontekstualnu svijest, moći će prenijeti više informacija. Primjerice, svjetionici će moći prenositi stvarni sadržaj umjesto da samo usmjeravaju sadržaj putem URL-a. Ovo može potencijalno redefinirati način na koji Bluetooth uređaji danas prenose informacije prelazeći prema IoT bez veze umjesto trenutnog modela uređaja s uparivim

Bluetoothom. Ovo također može učiniti BLE aplikacije poput praćenja imovine i pametnog upravljanja otpadom pametnijim mrežama pomoću BLE Mesh mreža.

No te poboljšane karakteristike zahtijevaju i poboljšani procesor u smislu DMIP-a i memorije. Podržani hardver (tj. SoC ili MCU) moraju se promijeniti kako bi podržali ove karakteristike. Sigurnost je ključna značajka koja se ne može pregovarati za većinu IoT aplikacija. Zaštita podataka potrebna je na svim razinama, uključujući pohranu, obradu i tokom komunikacije kako bi se osigurala pouzdanost sistema. IoT dizajneri radije odabiru SoC-ove koji imaju ugrađeni BLE, senzorska interfejse, sigurnosne karakteristike i fleksibilne periferne uređaje. Ovo im također pomaže da smanje prostor BOM i PCB za IoT uređaje.

Pogledajmo neke značajke koje BLE čine fleksibilnim i jednostavnim za upotrebu u IoT aplikacijama.

- **GATT profili**

BLE pruža nekoliko profila generičkih atributa (GATT) za tipične aplikacije koje pojednostavljuju upravljački softver i kriterije kompatibilnosti. Primjeri uključuju uslugu trenutnog vremena (CTS), pronađite profil (FMP), uslugu otkucaja srca (HRS), bežičnu kontrolu osvjetljenja (Mesh Profile), između ostalih. Ti profili omogućavaju perifernom uređaju i poslužitelju da međusobno komuniciraju koristeći unaprijed definirane podatkovne strukture s malim troškovima. To omogućuje BLE-u upotrebu jednostavnijih protokola od opcija povezivanja, poput Wi-Fi-ja. To također daje vrlo visoku učinkovitost prijenosa podataka. Ako vaša aplikacija odgovara postojećem GATT profilu, ne koristi ga jer ne smanjuje vrijeme razvoja softvera i otvara vrata postojećoj kompatibilnosti aplikacija. Popis standardnih GATT profila može se naći na web stranici BLE SIG.

Da biste dodatno pojednostavili postupak stvaranja upravljačkog softvera, IDE-ovi, poput Cypress-ovog ModusToolbox-a, pružaju grafički interfejs koji se jednostavno koristi za BLE. Ovi konfiguratori nude mogućnost dodavanja standardnih GATT usluga i konfiguriranja ih prije stvaranja firmvera kako bi događaji vezani uz uslugu mogli sami upravljati snopom. To znači da firmware za aplikacije jednostavno treba voditi računa o događajima na visokoj razini.

- **Prilagođeni profili**

U određenim aplikacijama možda će biti potrebno stvoriti prilagođene profile koji se ne pridržavaju postojećih standardnih GATT usluga. Primjeri uključuju prilagođena sučelja senzora, kapacitivno osjetljivo na dodir i RGB LED rasvjetu. Ova inovativna sučelja pomažu u integriranju mnogih funkcija pomoću jednog SoC-a i na taj način pružaju bolju snagu i uštedu troškova.

- **Potrošnja energije**

BLE je idealno rješenje za povezivanje male snage. Brzina prijenosa podataka može se isključiti za nižu snagu podešavanjem intervala povezivanja i veličine MTU (Maximum Transmission Unit). Integrirani BLE u sustav na čipovima omogućuje SoC-u da učinkovito koristi režim dubokog mirovanja, kao što smo raspravljali u 5. dijelu ove serije stupaca. SoC se može probuditi iz načina dubokog spavanja na BLE događajima i obrađivati podatke. Čak i pri visokim brzinama prijenosa podataka (do 2Mbps), BLE pruža znatne prednosti napajanja u odnosu na Wi-Fi za veze s niskom brzinom prijenosa podataka. Dvojezgreni SoC-ovi pružaju još veću fleksibilnost korištenjem popratne jezgre za BLE operacije staka, dok je glavni MCU slobodan za pokretanje softvera aplikacija, omogućujući sustavu da provede još više vremena u načinu dubokog mirovanja.

- **Emitovanje**

BLE je paket temeljen protokol s master / slave arhitekturom. Međutim, pruža način emitiranja bez problema, koji ne treba uparivanje. Način rada s emiterima mogu se koristiti "svjetionicima" za prenošenje poruka višestrukim slušaocima. Ova tehnologija omogućuje pametnim uređajima da izvršavaju određene radnje u blizini svjetionika. Uređaji dizajnirani za podršku svjetala trebaju biti vrlo niski jer je snaga jedan od glavnih zahtjeva za emitiranje. BLE lampice također mogu implementirati unutarnje mogućnosti praćenja lokacije.

- **Mesh umrežavanje**

Mesh umrežavanje postaje BLE izvan jednostavne arhitekture master / slave podržavajući više međusobno povezanih čvorova. To omogućava velikom broju IoT čvorova male snage (do 32767!) Da međusobno komuniciraju i eliminira potrebu za čvorištem / usmjerivačem. BLE Mesh implementira kontroliranu poplavnu mrežu s šifriranim i autentificiranim porukama. Osnovna veličina segmenta poruke je 11 bajtova, ali pomoću segmentacije i ponovnog sastavljanja može se proširiti na 384 bajta. Poruke imaju šifre, redoslijedne brojeve, vrijeme za život (TTL) te adrese izvora i odredišta. Adresiranje je fleksibilno i može se koristiti za označavanje pojedinog čvora ili grupe čvorova. BLE Mesh nudi i detaljnu provjeru autentičnosti s različitim vrstama tipki za mreže i specifične funkcionalnosti aplikacija. Pomoću BLE Mesh-a mreže se mogu premostiti na internetu putem pametnog telefona ili jeftinog premošćavajućeg uređaja, poput pametnog zvučnika, ili korištenjem kombinacije Wi-Fi / BT. U usporedbi sa ZigBee - vlasničkim mrežnim protokolom, BLE Mesh protokol pruža jeftin hardver i laganu stog protokola koji se temelji na poznatom Bluetoothu, koji donosi interoperabilnost s telefonima, računalima i postojećim BLE, BT i WiFi / BT uređajima.

Glavne razlike između Classic Bluetooth i BLE

između Classic Bluetooth i BLE postoji nekoliko ključnih razlika koje se ogledaju u dosegu, sigurnosti, latenciji, vremenskom lagu.

U narednom prikazu date su specifikacije ove dvije tehnologije gdje se možete bolje upoznati o njihovim ključnim razlikama i sličnostima

Prikaz: Razlike između Classic Bluetooth i BLE

Specifikacija	Classic Bluetooth	Bluetooth Low Energy (BLE)
Doseg	100m	Veći od 100m
Brzina prenosa podataka	1-3 Mbps	1 Mbps
Propusnost aplikacije	0,7-2,1 Mbps	0,27 Mbps
Frekvencija	2,4 GHz	2,4 GHz
Latencija	100 ms	6 ms
Time lag	100 ms	3 ms
Topologija mreže	Zvjezda	Zvjezda
Max potrošnja energije	Manja od 30 mA	Manja od 15 mA

Classic Bluetooth je fantastičan za proizvode koji zahtijevaju neprekidno strujanje glasa i podataka, poput:

- Bežične slušalice
- Prijenos datoteka između uređaja
- Bežične tastature i štampači
- Bežični zvučnici

Bluetooth niska energija (Bluetooth LE) idealno je prilagođena IoT aplikacijama kao što su:

- Uređaji slični fitbitu
- Senzori za nadgledanje

- Emiteri

Zaključno, Bluetooth Classic nije zastarjela verzija BLE. Bluetooth Classic i BLE istovremeno postoje i koriste se za različite aplikacije.

Sve zavisi od toga što pokušavate postići.

RFID

Radiofrekvencijska identifikacija (RFID) koristi radio valove za prijenos male količine podataka s RFID oznake na čitač unutar vrlo kratke udaljenosti. Do sada, tehnologija je omogućila veliku revoluciju u maloprodaji i logistici.

Vežući RFID oznaku na sve vrste proizvoda i opreme, kompaije mogu u stvarnom vremenu pratiti svoj inventar i imovinu - omogućavajući bolje planiranje zaliha i proizvodnje, kao i optimizirano upravljanje lancem opskrbe. Uz sve veće prihvaćanje IoT-a, RFID se nastavlja usavršavati u maloprodajnom sektoru, omogućujući nove IoT aplikacije poput pametnih polica, samokontrole i pametnih ogledala.

RFID tehnologija naširoko se koristi na mnogim poljima od praćenja goveda u pametnoj poljoprivredi do brojanja predmeta tijekom inventara skladišta. Maloprodaja, proizvodnja, logistika, pametno skladištenje i bankarstvo su jedne od glavnih industrija koje koriste RFID rješenja za IoT.

Šta je RFID tehnologija?

RFID, odnosno radiofrekvencijska identifikacija, tehnologija je koja koristi radio valove za omogućavanje komunikacije i prijenosa podataka između čitača i objekta koji ima posebnu oznaku pričvršćenu ili uklesanu. Ukratko, oznake odražavaju energiju koju emitira čitač i na taj način identificiraju objekt uz koji je spojen i prenose određene informacije poput lokacije.

Danas postoji veliki broj RFID oznaka. Na primjer, metalne oznake ugrađene su u metalni predmet i dizajnirane su da traju. RFID umetci omogućuju jednostavno lijepljenje oznake na površinu. Neke su oznake jeftine (oko 3 centa po komadu) i za jednokratnu upotrebu, druge su trajne i mogu doseći 20 USD po jedinici.

Tehnologija pasivne radiofrekvencijske identifikacije omogućava prepoznavanje objekta ili njegove lokacije na zahtjev. Naprednija verzija, Sustav lokacije u stvarnom vremenu (RTLS), podrazumijeva korištenje mreže čitača koji kontinuirano prate položaj označenih

objekata, postavljaju njihove lokacije na kartu te dinamički prate i prijavljuju sve promjene statusa.

Potencijali RFID tehnologije za primjenu u IoT

Primjena RFID tehnologije u IoT vrlo je široka i raznolika. RFID oznake primarno se koriste za međusobnu komunikaciju svakodnevnih predmeta i glavnog hub-a i izvještavanje o njihovom stanju. Na primjer, u zdravstvu, pokretna medicinska oprema s priloženim pasivnim RFID oznakama može se lako pronaći na dežurstvu.

RTLS omogućava praćenje označenih objekata u stvarnom vremenu i pomaže u stvaranju sustava povezanih uređaja koji kontinuirano prenose podatke o njihovoj lokaciji, uvjetima, količini itd. Ove mogućnosti čine osnovu za izgradnju IoT sustava. Drugim riječima, funkcija RFID tehnologije u IoT-u je povezati objekte u mrežu i natjerati ih na stvaranje i slanje podataka.

Ne samo podaci o statusu, ako govorimo o IoT i RFID nove generacije. Senzorski RFID oznake na akumulatorski pogon već se uveliko koriste u različitim područjima. Za razliku od jednostavnih RFID oznaka koje aktivno ne emitiraju signale, oznake s omogućenim senzorima mogu stvarati i slati metrike i druge podatke u stvarnom vremenu, proširiti mogućnosti povezanih uređaja i učiniti ih istinski pametnima.

Primjene tehnologije RFID-a usvojene su u mnogim uspostavljenim i novim zdravstvenim organizacijama, uključujući bolnice, laboratorije i privatne klinike.

Na primjer, dobro poznata Klinika Mayo implementirala je rješenje temeljeno na RFID-u na gastroenterološkom odjelu kako bi pratila uzorke tkiva pacijenta i osigurala da se podaci o pacijentu ne izgube ili registriraju pogrešno.

Medicinski centar Herzelia oslanja se i na RFID tehnologiju i koristi pametne ormare za automatizirani popis, nadzor uporabe i nadopunu proizvoda poput lijekova i medicinskih proizvoda.

Jedan od najboljih primjera RFID tehnologije dolazi od drugog vodećeg zdravstvenog pružatelja usluga iz SAD-a Kaiser Permanente. Koristeći razvoj RFID medicinskog uređaja za praćenje, tvrtka prati više od 140 000 pomičnih medicinskih uređaja i druge opreme za kontrolu uporabe i održavanja, optimizira rad zdravstvenih radnika i osigurava pravovremene usluge svih članova.

ZigBee

Šta je ZigBee?

ZigBee je specifikacija bežične lokalne mreže (WLAN) male snage koja je dizajnirana za pružanje malih količina podataka uz vrlo malo energije, a većina povezanih uređaja troši bateriju. Zbog toga je otvoreni standard povezan s komunikacijom mašina-mašina (M2M) i industrijskim internetom stvari (IIoT).

Za razliku od Wi-Fi-a, ZigBee koristi mesh specifikaciju mreže gdje su uređaji povezani s mnogim međusobnim vezama između drugih mrežnih čvorova. Podaci se uglavnom šalju na udaljenostima od srednjeg dometa od 10 do 100 metara, ali ZigBee koristi svoju mesh mrežu da bi značajno proširio tu udaljenost.

ZigBee temelji se na specifikaciji (IEEE) 802.15. Djeluje u nelicenciranim radio frekvencijskim opsezima, uključujući 2,4 GHz, 900 MHz i 868 MHz.

Slučajevi upotrebe za 802.15.4 usmjereni su na nadgledanje aplikacija u kojima je potrebna relativno niska razina protoka podataka, a uz mogućnost daljinskih senzora na baterije gdje je potrebna mala potrošnja energije. Senzori, aktuatori, kontrole osvjetljenja, sigurnosne i ostale kućne i građevinske aplikacije mogući su primjeri tehnologije.

- Karakteristike ZigBee protokola uključuju:
- Podrška za više mrežnih topologija poput point-to-point,
- mreže od točke do više točaka i mreže
- Niski radni ciklus - pruža dugo trajanje baterije
- Niska latencija
- Spektar širenja izravne sekvence (DSSS)
- Do 65.000 čvorova po mreži
- 128-bitna AES enkripcija za sigurne podatkovne veze
- Izbjegavanje sudara, ponovni pokušaji i potvrde

Izazovi i nedostaci

Zigbee vrlo dobro stoji u utrci da postane globalno prihvaćeni IIoT protokol.

Već se natječući s uspješnom konkurencijom poput Wi-Fi-ja i Bluetootha, kao i s novopridošlim Thread-om, prostor koji postaje rješenje za buduća IoT rješenja postaje sve veći.

Ali ZigBee već ima značajno mjesto na tržištu. Zapravo, ako posjedujete Nest termostat, Comcastov nedavni usmjerivač ili Hue žarulju, već imate ZigBee čipove u svom domu.

Nažalost, specifikacija je pala u teška vremena posljednjih godina, a problemi s interoperabilnošću ističu velik dio njenog pokrivanja. Problem je što standard nije samo bežični transportni mehanizam, već sloj softvera na vrhu koji može stvoriti profile koji ometaju različite verzije ZigBee profila. Dakle, za razliku od Wi-Fi-ja, ako imate dva uređaja sa ZigBee čipovima, moguće je da neće moći međusobno raditi.

Još jedan izazov koji ZigBee mora preuzeti je njegov najbliži konkurent, Z-Wave. Prema Gigaomu, otprilike devet od 10 senzora koristi zaštićeni Z-Wave standard preko ZigBee-a, a više startupa izlazi s Bluetooth uređajima s niskom energijom koji će komunicirati s mobilnim telefonima.

Prema Link Labsu dvije tehnologije imaju različite osobine koje ih međusobno razlikuju.

- ZigBee koristi globalno standardni opseg frekvencija od 2,4 GHz ISM. To znači da hardver nije specifičan za zemlju i da se može koristiti bilo gdje. Ovaj je opseg ponekad izložen prilično intenzivnim smetnjama od Wi-Fi i Bluetooth sustava.
- Z-Wave koristi iste opsege pod-GHz koje koristi Symphony Link, a to je u SAD-u 915 MHz ISM-opseg, a u Europi 868 MHz RFID-opseg.
- Mnogi pružatelji usluga proizvode ZigBee radio stanice, ali Z-Wave koristi vlasnički radio sustav Sigma dizajna. To nije nužno loše, jer Z-Wave pati od manje problema s interoperabilnošću nego ZigBee.
- Z-Wave koristi fizičku modulaciju s frekvencijskim pomicanjem (FSK), dok se ZigBee modulacija provodi kroz izravni sekvencijski šireni spektar (DSSS).

Mjesto ZigBee u IIoT

ZigBeeove karakteristike izdvajaju ga od ostalih mogućih IoT protokola i stavljaju ga u poziciju da pronađe svoje mjesto na tržištu. Mesh topografija znači da može podnijeti daljine veće od Bluetooth niskoenergetskih, a vrlo mala potrošnja energije čini je IoT-om omogućenijom od Wi-Fi-ja.

Prema Gigaomu, sljedeći korak nakon široke upotrebe čipova unutar domova bit će dobivanje ZigBee čipa unutar pametnih telefona. Budući da je mobilna slušalica ili tablet primarna metoda komuniciranja vlasnika kuće sa senzorima u kući, integriranje takvog

čipa stavilo bi ga u ruke milijuna vlasnika pametnih telefona koji bi ga mogli omogućiti pritiskom na gumb.

Trenutno se ZigBee radio prijemnici nalaze u domovima putem čvorišta, usmjerivača ili set top boxa - što njihovo usvajanje od strane vlasnika kuća ovisi o davateljima usluga i ranim korisnicima proizvoda poput Almond Routera, SmartThings čvorišta ili Revolv čvorišta.

Kompanije kao što su Comcast, Time Warner Cable, EchoStar, DirecTV, Charter, Rogers (Kanada), Deutsche Telekom i drugi implementirali su ZigBee tehnologiju koja omogućava njihove set-top box uređaje i satelitski primopredajnik za njihovu sigurnost, kontrolu kuće i energiju rješenja za upravljanje.

To je poticaj za usvajanje ZigBee-a, iako je ranije ove godine objavljeno da je utvrđeno da Comcast-ov sistem koji koristi protokol zasnovan na ZigBee-u za komunikaciju i rad u opsegu radio frekvencija od 2,4 GHz nije siguran.

ALDI INICIJATIVA ZA INOVATIVNI TRENING

Panorama b.b. 73 000 Goražde

Bosna i Hercegovina

INTERNET OF THINGS

DIZAJN I RAZVOJ APLIKACIJA

AITI-IOT-001-180-04

Dizajn i razvoj aplikacija

Povezivanje svih stvari u Internet of Things

AITI

Skill Accelerator

Follow us at @UAITLab

Dizajn i razvoj aplikacija

Povezivanje svih stvari u Internet of Things

Početkom 20 stoljeća nafta je bila glavni motor do tada neviđenog progresa i napredka širom svijeta. Sto godina kasnije nafti se bliži kraj (kako zbog ograničenih resursa tako i zvog negativnog uticaja na okoliš) mjesto ključnog resursa na kojem se zasniva razvoj sve više preuzimaju podaci koji su glavni motor četvrte industrijske revolucija (Industrija 4.0).

U predhodnom poglavlju imali ste prilike kako bi napravili dobru strategiju. I kao što ste mogli primjetiti, korištenje ovih alata skoro pa bezvrijedno bez odgovarajućih, tačnih i relevantnih podataka.

Kako bi bili u mogućnosti da skoristite puni potencijal podataka u ovom poglavlju su obrađene teme koje će vam pomoći da usvojite znanja iz oblasti poslovnog obavještanja (Business Intelligence) čija primjena doprinosi boljem, bržem i efikasnijem donošenju odluka, te će steći vještine rada sa podacima u softverskim platformama za provođenje analitike podataka u poslovne svrhe.

U ovom poglavlju vi će te se moći upoznati sa:

- Osnovama pristupa poslovnog obavlještavanja i novim pristupima korištenja poslovnih podataka u procesu donošenja odluka u organizaciji;
- Osnovama rada sa podacima kako bi mogli iskoristiti njihov puni potencijal za primjenu poslovne analike u upravljačkim procesima;
- Mogućnostima koje nude softverkse platfome Tableau i Power BI, dvije trenutno najbolje softverske platforme za poslovnu analitiku i Business intelligence za mala i srednja preduzeća/organizacije.

Znanje sa kom se možete upoznati u ovom poglavlju sigurno će vam olakšati napore na razvoju vaših strateških ideja. Međutim, oni vam takođe mogu biti od izuzetne koristi kada budete razvijali vaše prijedloge projekata putem vi vaše strateške ideje razrađujete u detaljne planove akcije.

Poslovna analitika u doba podataka postaje sve važniji alat koji se primjenjuje u poslovanju, zato ne gubimo vrijeme i krenimo da se upoznamo sa ovom jako zanimljivom temom.

1. Razvoj aplikacija pomoću IoT platforme

Osnove mrežnih tehnologije za IoT; IoT mrežni protokoli

Osnove IoT platformi

Razvoj i primjena IoT sistava je kompleksna oblast.

To je kompleksna oblast jer uključuje koordinaciju širokog spektra povezanih uređaja, mreža, Cloud usluga te mobilnih i web aplikacija.

IoT platforme olakšavanju ove kompleksnosti ponašajući se kao *middleware* (most između) za povezivanje i upravljanje IoT uređaja i podacima koje prikupljaju putem mobilnih i web aplikacija okrenutih prema korisnicima.

Ove IoT platforme obično su dizajnirane za uspostavljanje sigurne komunikacije između uređaja, aplikacija i usluga.

Važno je da razumijete da IoT platforme omogućuju i brži i lakši razvoj i implementaciju IoT aplikacija.

IoT platforme dizajnirane su da budu skalabilne i pouzdane.

Na primjer, primjenjuju toleranciju kvarova tako da će vaši IoT sustavi i dalje raditi u slučaju kvara uređaja, mreže ili usluga u Cloud-u. Koristeći standarde i pružajući dobro dokumentirane API-je i SDK-ove, IoT platforme omogućuju vam integraciju heterogenih uređaja, aplikacija i usluga u vaš IoT sistem, pružajući vam fleksibilnost za prilagodbu i zamjenu komponenata kako se zahtjevi mijenjaju.

Internet of Things razvija se brzim tempom, tako da ćete svoje IoT aplikacije trebati razvijati brzo i efikasno kako biste smanjili vrijeme za tržište i ostali konkurentni. Iako svaka IoT inicijativa dolazi sa svojim skupom jedinstvenih zahtjeva, većina IoT projekata dijeli neke zajedničke zahtjeve za upravljanje povezanim uređajima i komunikaciju, pohranu i analizu podataka koje generiraju.

IoT platforme rješavaju ove temeljne zahtjeve pružajući generičke, prilagodljive alate i usluge, kao i apstrakcije koje možete nadograditi kada razvijate svoja prilagođena IoT rješenja.

U ovom poglavlju mi ćemo istražiti ključne mogućnosti IoT platformi i uzimajući u obzir vrhunske IoT platforme opće namjene, shvatit ćete zašto biste trebali usvojiti IoT platformu za brzi razvoj svojih IoT rješenja i brzo dobivanje najviše vrijednosti iz vašeg IoT-a podaci.

Mogućnosti IoT platforme

IoT platforme olakšavaju razvoj IoT aplikacija zahvaljujući svojim brojim mogućnostima pomoću kojih možete upravljati uređajima, podacima, provoditi analitiku, integrisati komponente ili obezbjediti neophodnu sigurnost vašeg IoT projekta.

U ovoj sekciji obratićemo pažnju na ključne mogućnosti IoT platforme:

- Upravljanje uređajima
- Protokoli za komunikaciju podataka
- Pohrana podataka
- Pravila i analitika
- Brzi razvoj i primjena aplikacija
- Integracija
- Sigurnost
- Trošak razvoja i održavanja rješenja koja gradite pomoću IoT platforme.

Relativna važnost svake sposobnosti ovisi o zahtjevima vašeg projekta.

Na primjer, za mali sistem kućne automatizacije upravljanje uređajima nije primarna briga. U tim projektima je malo uređaja kojima se može upravljati. Kućna automatizacija uglavnom je reaktivna. Za IoT platformu manje je važno pružiti mogućnost pohrane podataka i analize podataka za pohranu i analizu povijesnih očitavanja senzora.

Međutim, IoT platforma mora podržavati brze i pouzdane protokole za podatkovnu komunikaciju kako bi osigurala da događaji koje senzori detektiraju ne budu propušteni i na njih reagirati u stvarnom vremenu. Pa ipak, za industrijsku IoT aplikaciju koja uključuje stotine senzora koji nadziru industrijsku opremu zbog kvarova, habanja i slabijih performansi, mogućnosti upravljanja uređajima i analitičke mogućnosti IoT platforme su mnogo važnije.

Hajdemo sada da se malo detaljnije upoznamo sa svakom od ovih izdvojenih mogućnosti IoT platforme.

Upravljanje uređajima

Jedna od osnovnih funkcija IoT platforme je upravljanje njezinim uređajima.

Upravljanje uređajima događa se tokom cijelog životnog ciklusa svakog IoT uređaja.

To uključuje osiguravanje novih uređaja, nadgledanje i održavanje operativnih uređaja i eventualno razgradnju uređaja na kraju njihovog korisnog vijeka trajanja.

IoT platforme omogućuju upravljanje registracijom uređaja, konfiguraciju i bežična ažuriranja. Uz odgovarajuću IoT platformu možete primati upozorenja o statusu uređaja i nadzirati analitiku i upotrebu uređaja te znati njegovo ukupno stanje i zdravlje.

IoT platforme mogu pružiti daljinsko ispravljanje pogrešaka kada stvari krenu po zlu. IoT platforme mogu također omogućiti upravljanje imovinom, uključujući mogućnost inventara i pronalaska povezanih uređaja i njihovih metapodataka.

Također je vrlo važno da IoT platforme budu "agnostičke na uređajima" i integriraju se s postojećim sustavima za planiranje resursa u poduzeću (ERP).

Protokoli za komunikaciju podataka

U predhodnom poglavlju imali ste priliku da se upoznate sa nekim od trenutno najzastupljenijim protokolima za komunikaciju podataka unutar ioT projekta. IoT platforme vam mogu jako dobro pomoći u njihovoj implementaciji.

Sigurna i pouzdana komunikacija između IoT uređaja, pristupnika i aplikacija i usluga temeljenih na oblaku ključni su za omogućavanje daljinskog upravljanja uređajima i njihovim vezama kako bi se osiguralo pravilno i kontinuirano prikupljanje i prijenos podataka.

Iako se neki podaci mogu lokalno pohraniti i obraditi rubnom analitikom, mnogo podataka koji se prikupljaju daljinski pomoću senzora i drugih IoT uređaja.

Stoga će usluge i aplikacije u oblaku uzvodno biti potrebne za potrebno agregiranje, obradu, pa čak i vizualizaciju. Hiljade uređaja često su povezane u jedan IoT sistem, a mnoge IoT platforme uključuju usluge posredovanja poruka kako bi uređaji i pristupnici mogli slati i primati poruke s malim kašnjenjem i u velikom opsegu.

Te usluge posrednika poruka obično koriste standardne komunikacijske protokole poput MQTT, CoAP ili XMPP, dok neke platforme podržavaju web utičnice za komunikaciju u stvarnom vremenu.

Pohrana podataka

S hiljadama povezanih uređaja koji generiraju podatke bez presedana, mjesto za pohranu golemih količina podataka još je jedna od važnosti pri odabiru IoT platforme. IoT platforme vam omogućavaju da kreirate i razvijete „Data lake“ u kojima možete pohraniti podatke u različitim formatima, uključujući neobrađene, polustrukturirane ili strukturirane.

Ta se „jezera podataka“ često grade na vrhu NoSQL ili Hadoop tehnologija radi maksimalne fleksibilnosti i skalabilnosti. Jezera podataka i druge pohrane podataka visoko su dostupne, podržavaju istodobna čitanja i upisivanja i uključuju konfigurabilne indekse za poboljšanje performansi kada vaša IoT aplikacija pristupa podacima i traži ih.

Pravila i analitika

Nakon što se podaci pouzdano pohrane, morate ih moći analizirati.

Mnoge IoT platforme nude analitičke mogućnosti koje uključuju obradu u realnom vremenu i u limitiranoj količini ili broju (eng. batch processing).

Mehanizam pravila izvodi analitiku podataka u stvarnom vremenu za uvide koji se mogu iskoristiti za donošenje odluka vas kao rukovodioca projekta ili vaših krajnjih korisnika.

Pravila koja kodiraju uvjete pokreću radnje.

Neke platforme nude aplikacije za analitiku po sistemu "ključ u ruke". Ostale platforme nude fleksibilnost za prilagodbu izvještaja, analitike, nadzornih ploča i vizualizacija podataka.

Brzi razvoj i primjena aplikacija

Brzina razvoja i isporuke namjenskih aplikacija ključna je briga za IoT platformu.

Odaberite IoT platformu koja nudi alate za generiranje uzorka koda, predloške ili widgete za brzi razvoj te alate za pojednostavljivanje i automatizaciju implementacije.

Integracija

Interoperabilnost je još jedno važno razmatranje.

Postoji široka paleta povezanih uređaja i usluga povezanih s IoT-om. Milijarde IoT uređaja će biti na mreži tokom sljedećih nekoliko godina.

Bitna je brza provjera vašeg IoT sistema u budućnosti.

IoT platforme postižu ovu interoperabilnost usvajanjem standarda i pružanjem dodatnih slojeva apstrakcije i normalizacije u odnosu na osnovne tehnologije. Na primjer, manje je vjerojatno da će se vaše aplikacije pokvariti

Sigurnost

Sigurnost je sastavni dio dizajna bilo kojeg IoT rješenja.

Sigurnost uključuje zaštitu uređaja i mreža uz sigurnost u oblaku i na razini aplikacija. Odaberite IoT platformu koja pruža usluge provjere autentičnosti i autorizacije, po mogućnosti s integracijom, postojećim sustavima koji se koriste za upravljanje identitetima poput LDAP-a.

Razmislite o usvajanju standarda kao što je X.509 za provjeru autentičnosti uređaja.

Za sigurnu komunikaciju usvojite standard poput TLS-a za šifriranje sadržaja i osiguravanje integriteta podataka. IoT platforme također mogu implementirati kontrolu pristupa zasnovanu na ulogama za korisnike, uređaje, pristupnike i usluge, kao i pružanje alata za nadzor i reviziju sigurnosti.

Trošak

Ubrzanje razvoja IoT rješenja jedna je od glavnih blagodati usvajanja IoT platforme, no IoT platforma također može pomoći u smanjenju troškova razvoja.

Tekući troškovi, poput pretplata za pristup hostiranoj IoT platformi ili troškovi hostinga za samo hostiranu platformu, obično će biti manji od troškova razvoja i održavanja vlastitih rješenja po mjeri.

Mnoge IoT platforme nude besplatna probna razdoblja ili razine niske upotrebe koje možete upotrijebiti za početak bez gotovo troškova unaprijed, ali budite sigurni da ćete uzeti u obzir kako će se ti troškovi promijeniti nakon završetka početnog probnog razdoblja.

Usporedba IoT platformi

Postoje stotine IoT platformi dostupnih od različitih dobavljača. Neke su platforme visoko specijalizirane, na primjer, poslužuju samo jednu tržišnu vertikalu poput GE Predix-a (https://www.predix.io/), PaaS IoT platforme koja je posebno usmjerena na industrijski IoT.

Ostale IoT platforme usredotočene su na pružanje samo podskupa funkcija koje bi mogle biti potrebne za vaš IoT projekat, umjesto na cjelovito rješenje IoT platforme, na primjer, Cisco i SAS Edge-to-Enterprise IoT Analytics platforma, koja usredotočena je samo na IoT analitiku.

Kao rezultat toga, možete odlučiti usvojiti više od jedne IoT platforme.

Kao početnu točku evo pet popularnih IoT platformi opće namjene od kraja do kraja koje su prikladne za širok spektar primjena:

IBM Watson IoT

Izgrađen na vrhu IBM Cloud platforme, IBM Watson IoT je zrela IoT platforma prilagođena programerima s prednostima u analitici u realnom vremenu i kognitivnom računanju.

Platforma također podržava upravljanje uređajima, provjeru autentičnosti i autorizaciju, sigurnu pohranu podataka i komunikaciju, standardne komunikacijske protokole poput MQTT i HTTPS, pravila, REST API-je i SDK-ove.

Prema IDC-u, kompanije za istraživanje tržišta, portfelj Watson IoT i Watson IoT platforma nazvani su IoT platforma platformi.

Amazon Web Services IoT

AWS IoT je visoko skalabilna IoT platforma.

Sadrži SDK, provjeru autentičnosti i autorizaciju, registar uređaja, pristupnik uređaja koji komunicira s uređajima koji koriste MQTT, WebSockets ili HTTP i mehanizam pravila koji se integrira s postojećim AWS uslugama poput DynamoDB.

Zanimljiva karakteristika AWS IoT-a je "sjene uređaja", koja je postojana virtualna verzija svakog uređaja, uključujući posljednje poznato stanje uređaja.

Microsoft Azure IoT Suite

Microsoft Azure IoT Suite još je jedna sveobuhvatna IoT platforma koja uključuje podršku za upravljanje uređajima i blizance uređaja (poput zasjenjivanja uređaja) korištenjem Azure IoT Hub-a, standardnih komunikacijskih protokola, uključujući MQTT, AMQP i HTTP, sigurnu pohranu, pravila i alate za analizu podržavajući prediktivnu analizu i vizualizaciju podataka.

ThingWorx

PTC ThingWorx je poslovna IoT platforma koja podržava brzi razvoj aplikacija na temelju modela. Značajke uključuju upravljanje uređajima, modeliranje aplikacija, podršku za

standardne protokole, uključujući MQTT, AMQP, XMPP, CoAP i WebSockets te prediktivnu analitiku, kao i REST API-je i SDK-ove za podršku integraciji.

Kaa

Kaa je besplatna IoT platforma s otvorenim kodom koja je objavljena pod licencom Apache 2.0, što omogućuje samostalno hostiranje platforme.

Kaa uključuje REST API-je i SDK-ove za Javu, C ++ i C, sa značajkama za upravljanje uređajima, prikupljanje podataka, upravljanje konfiguracijom, obavijesti, uravnoteženje opterećenja i analizu podataka.

2. Watson IoT Platforma

Pregled Watson IoT platforme; Započinjanje sa radom u Watson IoT Platformi; Korištenje Watson IoT Platform Dashboard;

Pregled Watson IoT platforme

IBM® Watson ™ IoT platforma temelji svju ponudu na IBM Cloud-u koja može povezati i kontrolirati IoT senzore, uređaje, domove i industriju.

Izgrađena na IBM Cloudu, Watson IoT Platform pruža opsežni skup ugrađenih i dodanih alata. Vi možete upotrijebiti ove alate za obradu IoT podataka u stvarnom vremenu i povijesnom analitikom, izvući ključne pokazatelje uspješnosti (KPI) iz svojih podataka, dodajte „pamet“ u Cloud za pametne proizvode i da sigurno povežete vlastite aplikacije i postojeće alate s Infrastruktura platforme Watson IoT.

Rešenje IBM® Watson ™ IoT Platforma pruža skup IBM Cloud usluga kao jedinstvenu SaaS-ovu ponudu kojom upravlja IBM koja vam omogućava prikupljanje i analizu relevantnih podataka o performansama proizvoda i korištenju za vaše imovine omogućene IoT-om.

Ključne karakteristike

Sljedeće ključne značajke uključene su u rješenje Watson IoT Platform:

- **Povezivanje**

Unos IoT podataka u obliku MQTT događaja iz bilo kojeg izvora pomoću Platform Service za registraciju, povezivanje i upravljanje vašim IoT uređajima. Uz to, karakteristika povezivanja omogućuje vašim aplikacijama i IBM Cloud uslugama pretplatu na te događaje za obradu podataka događaja. Uključeni su i ostali API-ji za registraciju uređaja, upravljanje i još mnogo toga.

- **Snimanje podataka**

Watson IoT vam omogućava da pohranjujete svoje IoT podatke kratkoročno u Cloudant NoSQL DB rješenje, koje vam daje direktan pristup podacima u posljednjih 30 dana za vaše uređaje. Na isti način, koristite IBM® Streaming događaja za IBM Cloud za direktan pristup nedavnim podacima.

- **Monitoring**

Ova platforma vam omogućava da kreirate pregled svoje imovine i entiteta s ugrađenim dashboard-ima za nadzor. Njih možete koristiti kako biste linijskim poslovnim korisnicima omogućili praćenje stanja IoT entiteta.

- **Analiziranje**

Vrlo važna karakteristika Watson IoT jeste mogućnost korištenja ugrađenih i eksternih alata za sortiranje podataka, sažimanje, Machine learning i još mnogo toga. Vi možete koristiti analitičke usluge kako biste linijskim poslovnim korisnicima omogućili jednostavno obogaćivanje i interakciju sa sirovim podacima mjernih podataka koji dolaze iz IoT uređaja pomoću ugrađenih konfigurabilnih funkcija analitike.

- **Arhiva**

Watson IoT vam omogućava da prilagodite svoje mogućnosti pohrane i upravljanje životnim ciklusom podataka pomoću priloženog rješenja za dugoročno pohranu, IBM® Cloud Object Storage.

- **Upravljanje i nadgledanje upotrebe**

Watson IoT Platform SaaS rješenjem upravlja se kao jedinicom, s punim statusom i vezom preko nadzorne ploče Watson IoT Platform. Pristupite svojim uslugama na razini korisnika uz sigurnost sustava.

Za nadgledanje upotrebe možete koristiti nadzornu ploču Watson IoT za praćenje potrošnje i upotrebe podataka za svaku uključenu uslugu na vašem računu kako biste ispravno odredili vaše potrebe za rješenjem. Surađujte s timom IBM IoT Solutions DevOps kako biste rješenje prilagodili svojim organizacijskim potrebama.

Sa Watson IoT ™ platformom vi možete započeti sa malim projektom koji se brzo može razviti i lako možete da se povežete sa IoT uređajima, sakupljati i obrađivati IoT podatke brzo i jednostavno. Obzirom da se koristi IBM Cloud, vaš projekat se brzoo može brzo prilagoditi promjenjivim poslovnim potrebama bez ugrožavanja sigurnosti, privatnosti ili razine rizika.

Posebna je prednost što možete koristiti uslugu analitike za vizualizaciju i AI analitiku u oblaku. Omogućuje vašoj djelatnosti proširivi katalog analitičkih funkcija za obogaćivanje, proširivanje i na kraju stjecanje uvida u podatke na jednostavan i intuitivan način.

Arhitektura IBM® Watson ™ IoT platforme

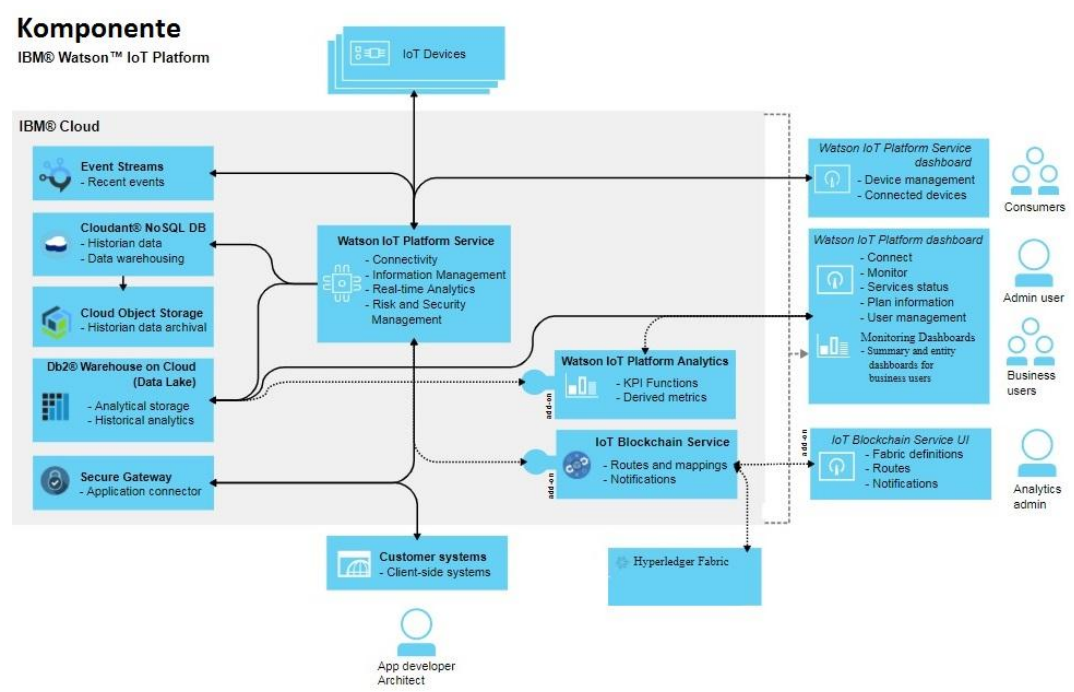
IBM® Watson ™ IoT platforma je cjelovita, potpuno upravljana usluga u oblaku koja integrira skup unaprijed odabranih usluga kako bi formirala javno, multitenantno SaaS rješenje na IBM Cloud okviru.

IBM Cloud usluge koje čine Watson IoT Platform pružaju podršku glavnim funkcijama proizvoda povezivanja, spremanja, analiziranja i upravljanja uz daljnju podršku praćenja putem nadzorne ploče Watson IoT Platform.

IBM Cloud framework, kojim upravlja tim IBM IoT Solutions DevOps, upravlja pozadinskim operacijama, poput sigurnosti, raspodjele resursa, sigurnosne kopije i velike dostupnosti.

Pregled komponenti Watson IoT platforme dat je na slijedećem prikazu.

Prikaz: Watson IoT komponente



Prikaz: Pojašnjenja pojedinih komponenti Wastson IoT platforme

Usluga	Detalji	Pristup
Platform Service	Sigurna, pametna, skalabilna usluga platforme koja se koristi kao posrednik poruka IoT uređaja za sigurnu registraciju uređaja, analitiku u stvarnom vremenu i još mnogo toga.	Nadzorna ploča, nadzor nadzornih ploča, API, integracija aplikacija, integracija IBM Cloud usluga
Analytics Service (add-on)	Dodatna komponenta koja proširuje funkcionalnost IBM® Watson ™ IoT platforme tako da uključuje analitičke značajke. Poslovni korisnici mogu koristiti uslugu Analytics za interakciju s njihovim IoT podacima i izvođenje bitnih pokazatelja uspješnosti.	Dashboard, API
IoT Registration Service	Usluga za održavanje registra IoT uređaja i potrošača i njihovo neometano povezivanje	Registration UI in Platform Service dashboard, API
Watson IoT Platform starter	Demonstracijska aplikacija temeljena na Node.js koja prikazuje registraciju uređaja, mapiranje potrošača, kontrolu uređaja i još mnogo toga. Pokretač uključuje uzorak aplikacije, uzorak mobilne aplikacije i skup uzorka Node-RED protoka. Važno: Pokretač Watson IoT Platform dostupan je samo u neproizvodnom okruženju. Za više informacija, pogledajte preglednu temu ili kontaktirajte imenovanog administrativnog kontakta za vašu IBM uslugu.	Starter API, Sample app web console, Mobile app
Cloudant NoSQL DB	Upravljana usluga baze podataka NoSQL koja bilježi mjerenja i događaje uređaja i pohranjuje ih za uporabu u aplikacijama u stvarnom vremenu. Domaćin i potpuno upravljana baza podataka kao usluga (DBaaS) koja obrađuje razne vrste podataka, poput JSON-a, punog teksta i geoprostornih. Automatsko generiranje sheme i agregiranje podataka uređaja. Kombinirajte poslovne podatke s podacima o uređajima.	API, IoT Platform integration
Db2® Warehouse on Cloud	Podatkovno jezero Watson IoT Platform. Pohrana srednje veličine i analitika vaših IoT podataka. SQL baza podataka zasnovana na oblaku koja uključuje Netezza® tehnologiju za robusne analitičke mogućnosti.	Dashboard, Clients, API
IBM® Cloud	Nestrukturirana pohrana podataka u oblaku za	API, Watson IoT

Usluga	Detalji	Pristup
Object Storage	dugotrajno čuvanje. Skalabilna i potpuno upravljana pohrana. Međuregionalno i regionalno otporno.	Platform Dashboard (Bucket creation)
IBM Cloud App ID	Autentifikacija za mobilne i web aplikacije koje se povezuju s vašim rješenjem Watson IoT Platform. Podržava provjeru autentičnosti za Facebook i Google+.	OAuth server, Access via IBM support.
IBM® Secure Gateway for IBM Cloud	Siguran način pristupa lokalnim podacima ili podacima u oblaku iz vaše IBM Cloud aplikacije korištenjem sigurnog prolaza.	Contact IBM support to configure.
IBM® Event Streams for IBM Cloud	Skalabilna sabirnica poruka velike propusnosti. Povežite mikro-usluge koristeći otvorene protokole. Povežite stream podatke s analitikom kako biste ostvarili snažne uvide. Pošaljite podatke o događajima u više aplikacija kako bi reagirali u stvarnom vremenu. Premostite svoju lokalnu infrastrukturu za razmjenu poruka kako biste stvorili hibridno rješenje za razmjenu poruka u oblaku.	Watson IoT Platform Dashboard (Message creation), Admin API, Kafka REST API

Skladištenje IoT podataka

Watson IoT platforma prikuplja i zadržava IoT podatke za direktan pristup i obradu, a također i za pohranjivanje i arhiviranje u tri odvojene baze podataka.

Watson IoT Platforma uključuje niz zasebnih rješenja za pohranu podataka za zadržavanje IoT podataka za različite svrhe i vremenska razdoblja.

Koriste se sljedeće baze podataka:

- **Cloudant NoSQL DB** Najnoviji istorijski podaci za vaše IoT uređaje. Pogledajte trendove na pločama i karticama Platform Service.
- **IBM® Event Streams for IBM Cloud.** Trenutni i nedavni povijesni podaci za vaše IoT uređaje.
- **Db2® Warehouse on Cloud - Analytics Service data lake**. Dugoročni povijesni podaci za pristup analitici. Koristite analitičke alate za izvlačenje znanja iz svojih podataka. Ako vaš plan uključuje dodatak usluge Google Analytics, Db2® Warehouse on Cloud čini jezero podataka iz kojeg se troše podaci entiteta i na koje se zapisuje izlaz.

- **IBM® Cloud Object Storage** Kompletni skup povijesnih podataka za arhivske svrhe. Lokalno preuzmite podatke za izvanmrežnu obradu.

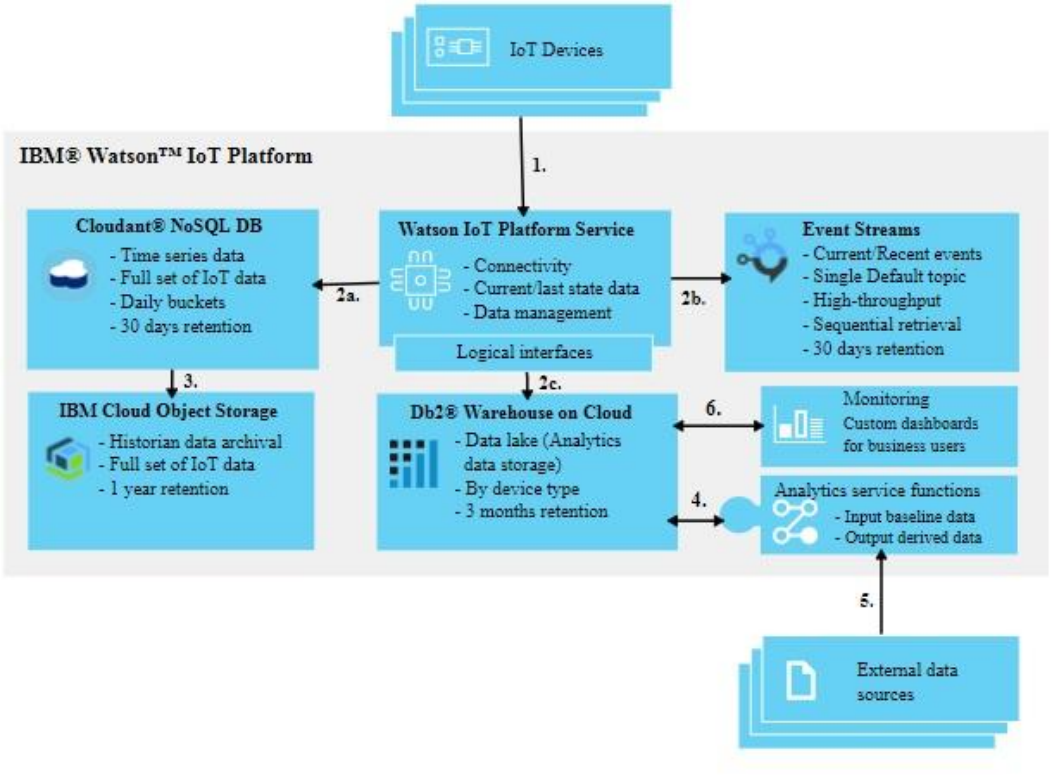
Protok IoT podataka

Watson IoT platforma koristi sljedeći protok podataka IoT uređaja:

1. Vaši IoT uređaji šalju podatke Platform Serviceu, koji djeluje kao posrednik poruka i rukovatelj IoT podacima u stvarnom vremenu. Da bi podaci vašeg IoT uređaja bili dostupni Watson IoT platformi, morate se registrirati, povezati i stvoriti blizanac uređaja za svoj uređaj u usluzi Platform.
2. Podaci uređaja zapisuju se na:
    a. Cloudant NoSQL DB za kratkoročni pristup povjesničara.
    b. IBM® Event Streams for IBM Cloud za sekvencijalno preuzimanje trenutnih i nedavnih podataka uređaja u stvarnom vremenu. Važno: Integracija Watson IoT platforme s IBM® događajima za IBM Cloud trenutno podržava samo objavljivanje poruka na jednu zadanu temu za sve vrste uređaja.
    c. Db2® Warehouse on Cloud za pohranu i analitiku srednje dužine. Važno: Da bi se podaci uspješno slijevali u Db2 Warehouse na Cloud, pobrinite se da su ispunjeni sljedeći zahtjevi: Logično sučelje za stvaranje potrebnih tablica i unos IoT podataka. Za više informacija pogledajte Pretvaranje uređaja u logičke cjeline. Korisni teret poruke mora ispunjavati zahtjeve koji su navedeni u podatkovnoj komponenti IBM® Db2® Warehouse on Cloud.
3. Cjelokupni skup podataka također se zapisuje u IBM® Cloud Object Storage za dugoročno pohranjivanje.
4. Dodatak usluge Analytics: Analitička komponenta koristi Db2® Warehouse on Cloud kao podatkovno jezero iz kojeg se troše podaci entiteta i na koje se zapisuje izlaz funkcije.
5. Dodatak usluge Analytics: uvoz i unos podataka o entitetima iz vanjskih izvora.
6. Konzumirajte podatke o entitetima pomoću prilagođenih nadzornih ploča za nadzor.

Protok podataka grafički je prikaazan na narednoj slici.

Prikaz: Protoko podataka u Watson IoT



Zadržavanje IoT podataka

Svako rješenje za pohranu ima različito zadano razdoblje čuvanja IoT podataka.

U zavisnosti od opcije plana korištenja IBM IoT, poput broja uređaja i veličine poruke, stopa zadržavanja vašeg rješenja može se razlikovati od sljedećih zadanih stopa plana. Čišćenje podataka slijedi ciklus zadržavanja i događa se svakodnevno, s jednim cjelodnevnim čišćenjem podataka u ponoć za svaku opciju pohrane.

Važno: Zadržavanjem podataka funkcije usluge Analytics ne upravlja proces životnog ciklusa podataka IoT. Umjesto toga, kada deaktivirate aktivnu funkciju, svi se njezini podaci uklanjaju iz podatkovnog jezera.

Prikaz: Opcije čuvanja i brisanja podataka u Watson IoT

Opcija skladištenja	**Čuvanje podataka o pohrani**	**Čišćenje podataka**
Cloudant NoSQL DB	30 dana	Podaci se pohranjuju i svakodnevno čiste od baze podataka do baze

		podataka.
IBM® Event Streaming for IBM Cloud	30 dana	Podaci se pohranjuju i pročišćavaju svakodnevno
Db2® Warehouse on Cloud	3 mjeseca	Podaci se čiste red po red, a shema ostaje ista
Database for PostgreSQL	3 mjeseca	Podaci se čiste red po red, a shema ostaje ista
IBM® Cloud Object Storage	1 godina	Podaci stariji od ograničenja zadržavanja svakodnevno se brišu

Da biste promijenili stopu zadržavanja komponenata za pohranu, kontaktirajte svog predstavnika IBM-a koji je naveden u pozdravnom pismu vaše IBM® Watson ™ IoT platforme.

Backup podataka

Pri radu sa bilo kojom IoT platformom važno je da znate koja vrsta podataka se sigurnosno kopira (Backup).

Sljedeće vrste podataka klijenta trenutno su sigurnosno kopirane kao dio strategije usluge platforme:

- Informacije o organizaciji
- Informacije o uređaju
- API ključevi i tokeni
- Informacije o korisniku
- Svi zapisi zahtjeva za upravljanje uređajima, uključujući povijest svih pokrenutih zahtjeva - na primjer trenutno stanje zahtjeva
- Definicije prilagođenih snopova zahtjeva za upravljanje uređajima
- KPI konfiguracije

Koja vrsta podataka nema sigurnosnu kopiju?

Sljedeće vrste podataka nisu sigurnosno kopirane u usluzi Platform:

- Događaji na uređaju
- Prijelazno stanje poruka, na primjer podaci tijekom leta
- MQTT poruke koje se šalju i primaju kao dio zahtjeva za upravljanje uređajem
- Izračunate metrike

Mjerene

Planovi usluga usluge plaćene platforme (planovi koji nisu IBM Cloud Lite plan) temelje se na konceptu megabajta razmijenjenih tijekom mjeseca. Ovaj dokument detaljno opisuje kako Platform Service mjeri podatke kako bi stvorio informacije o korištenju koje određuju cijenu korištenja usluge. Podaci o upotrebi mogu se koristiti za približne troškove korištenja usluge platforme na temelju dizajna i broja uređaja, aplikacija i pristupnika.

- **Podaci razmijenjeni**

Izračun razmijenjenih podataka uključuje podatke o računu koje aplikacije, uređaji i pristupnici razmjenjuju pomoću MQTT ili HTTP poruka i podatke koje aplikacije razmjenjuju pomoću HTTP API-ja.

- **MQTT podaci razmijenjeni**

Kada se koristi MQTT, sadržaj TCP protoka računa se na razmijenjene podatke. Korisni teret bilo koje MQTT poruke uključen je u kumulaciju podataka koji se razmjenjuju pomoću MQTT protokola. Kumulacija veličine podataka o korisnom opterećenju događa se kada je poruka objavljena, kao i kada je poruka dostavljena pretplatniku.

MQTT protokol dizajniran je da bude što lakši. Iako usluga platforme uključuje veličine MQTT paketa prilikom kumulacije razmijenjenih podataka, jer je to lagani protokol, ovi režijski troškovi su mali. Sljedeća tablica daje naznaku minimalne veličine svakog MQTT paketa:

Prikaz: Minimalna veličina svakog MQTT paketa

MQTT PACKET	Minimum size bytes	Variables and associated minimum size in bytes
CONNECT	56	Client ID (12 if d:xxxxxx:t:i), will topic (0) and will message (0) if set, username (14 for devices - 'use-token-auth') and password (18 if auto-generated)
CONNACK	4	Nothing

MQTT PACKET	Minimum size bytes	Variables and associated minimum size in bytes
PUBLISH	21	Topic name (17 if iot-2/evt/i/fmt/f) and payload (0 is the minimum). Applies to both inbound and outbound PUBLISH packets.
PUBACK	4	Nothing
PUBREC	4	Nothing
PUBREL	4	Nothing
PUBCOMP	4	Nothing
SUBSCRIBE	26	Can include multiple of both topic filter (19 if iot-2/evt/i/fmt/f) and QoS (1)
SUBACK	5	(1) for every topic filter in SUBSCRIBE
UNSUBSCRIBE	23	Can include multiple topic filters (19 if iot-2/evt/i/fmt/f)
UNSUBACK	4	Nothing
PINGREQ	2	Nothing
PINGRESP	2	Nothing
DISCONNECT	2	Nothing

Kada se koristi TLS, također se razmatra sigurno rukovanje. Rukovanje je približno 8 kilobajta. Stoga je isplativije MQTT veze držati otvorenima što je duže moguće. Otvorene veze imaju samo režijske troškove PINGREQ i PINGRESP (4 bajta) po intervalu održavanja, koji je specifičan za klijenta i ovisi o navedenom razdoblju održavanja. Ponovnim otvaranjem TLS veze upotrebom postojeće TLS sesije smanjuje se broj bajtova koji se razmjenjuju jer se certifikati ne šalju ni u jednom smjeru. Mnogi TLS klijenti to podržavaju prema zadanim postavkama, ali sesija ima ograničeni vijek trajanja. Korištenje klijentskih certifikata povećava veličinu TLS rukovanja, ovisno o veličini klijentskog certifikata.

TLS zapisi i TCP i IP opći troškovi se ne uzimaju u obzir.

Napomena: Kada se za pregled uređaja koristi nadzorna ploča usluge Platform, vrši se pretplata na MQTT tako da nadzorna ploča može prikazivati događaje uživo. Ova pretplata na MQTT također se računa u ukupnu količinu razmijenjenih podataka.

Razmijenjeni podaci o HTTP porukama

Kada se koristi HTTP poruka, korisni teret poruke uključuje se u kumulaciju razmijenjenih podataka, kako prilikom objavljivanja događaja ili primanja naredbi.

Kao i kod MQTT-a, HTTP režijski troškovi se broje. HTTP režijski troškovi znatno su veći od MQTT općih troškova. HTTP režijski iznos po zahtjevu iznosi približno 300 bajtova. Potrebno je dodati i veličinu korisnog tereta poruke.

Kada se koristi TLS, razmatra se sigurno rukovanje. Rukovanje je približno 8 kilobajta. Stoga je isplativije HTTPS veze držati otvorenima što je duže moguće. Otvorene veze ne uključuju dodatne troškove u pogledu razmjene podataka. Ponovnim otvaranjem TLS veze upotrebom postojeće TLS sesije smanjuje se broj bajtova koji se razmjenjuju jer se certifikati ne šalju ni u jednom smjeru. Mnogi TLS klijenti to podržavaju prema zadanim postavkama, ali sesija ima ograničeni vijek trajanja. Korištenje klijentskih certifikata povećava veličinu TLS rukovanja, ovisno o veličini klijentskog certifikata.

TLS zapisi i TCP i IP opći troškovi se ne uzimaju u obzir.

Razmijenjeni podaci HTTP API-ja

Kada se aplikacija pozove na bilo koji API, i zahtjev i tijela za odgovor kumuliraju se prema razmijenjenim podacima. Veličine svake mogu se značajno razlikovati, ovisno o API-ju.

Za razliku od MQTT i HTTP poruka, ni HTTP režijski ni TLS režijski podaci ne uzimaju se u obzir za razmijenjene podatke HTTP API-ja.

Napomena - Kada se koristi nadzorna ploča Platform Service, nadzorna ploča koristi HTTP API-je za popis podataka u uređajima za uključivanje, vrstama uređaja i zapisnicima veza uređaja. Ovi HTTP API pozivi računaju se na razmijenjene podatke.

Započinjanje sa radom u Watson IoT platformom

IBM® Watson ™ IoT platforma cjelovito je rješenje za vaše IoT potrebe. Integrira paket usluga za povezivanje, snimanje, registraciju, analizu i arhiviranje vaših IoT uređaja i podataka.

Prije nego što počnete raditi s Watson IoT Platformom, morate imati instaliranu, konfiguriranu i pokrenutu instancu usluge. Proizvod dolazi s nekoliko različitih planova rješenja koji se temelje na vašim potrebama, uključujući neproizvodno rješenje koje dolazi s uzorkom aplikacije i pruža izvrsno polazište za upotrebu i razvoj Watson IoT platforme. Za više informacija i kontaktiranje IBM-ove prodaje, pogledajte Watson IoT Platform na IBM Marketplace.

Koraci za brzi početak

Sljedeći koraci opisuju kako možete brzo započeti s Watson IoT Platformom. Zbog prirode Watson IoT platforme, ovaj vodič za početak sadrži uglavnom opise koraka i zadataka koje možete izvoditi na visokoj razini. Za svaki korak nalaze se poveznice na detaljnije informacije.

Korak 1: Napravite pregled Watson IoT platforme

Kada je vaša instanca Watson IoT Platform dostupna, možete joj pristupiti i započeti istraživanje uključenih usluga pomoću nadzorne ploče Watson IoT Platform.

Savjet: Da biste pristupili nadzornoj ploči Watson IoT Platform, upotrijebite URL i podatke za prijavu koji se nalaze u pozdravnom pismu vašeg IBM® Watson ™ IoT Platform. Ako nemate pristup pozdravnom pismu, kontaktirajte svog lokalnog administratora Watson IoT platforme. Možda ćete također trebati kontaktirati svog administratora da vas doda kao korisnika nadzorne ploče.

Na kartici Usluge nadzorne ploče usluge Watson IoT Platform vidite popis usluga koje su uključene u vašu organizaciju Watson IoT Platform. Te se usluge razlikuju prema planu rješenja.

Važno: Sve uključene usluge konfigurirane su i spremne za rad od početka, ali neke će možda trebati daljnju konfiguraciju. Na primjer, morate povezati uređaje s uslugom platforme da biste mogli vidjeti podatke o IoT uređajima kako pristižu.

Nadzorna ploča Watson IoT platforme također vam omogućuje praćenje podataka i upotrebu obrade u svim uslugama, pregledavanje najava i obavijesti, upravljanje pristupom nadzornim pločama i još mnogo toga.

Korak 2: Povežite uređaje

Prije nego što počnete primati podatke sa svojih IoT uređaja, prvo se morate registrirati i povezati ih sa svojim okruženjem Watson IoT Platform, a zatim stvoriti sučelja za upravljanje podacima s kojima se Watson IoT Platform može povezati.

Savjet: Ako nemate uređaje koji su spremni za povezivanje, možete poslati uzorke podataka pomoću Python simulatora ili upotrijebiti ugrađeni simulator uređaja Platform Service da biste započeli testiranje platforme Watson IoT.

Korak 3: Prikaz IoT podataka u stvarnom vremenu

Nakon što potvrdite da podaci uređaja pristižu u uslugu platforme, također želite potvrditi da se podaci mogu vidjeti u IBM® događajima za IBM Cloud za blisku upotrebu

u stvarnom vremenu i da su zapisani u IBM® Cloudant® NoSQL DB za IBM Cloud za kratkoročnu povijesničku analizu.

Možete koristiti Streamove događaja i Cloudant® NoSQL DB podatke, na primjer, za pokretanje pravila i radnji te za stvaranje "živih" korisničkih sučelja.

U ovom koraku koristite nadzornu ploču Watson IoT Platforme za prijavu na svoju nadzornu ploču Cloudant® NoSQL DB i za dobivanje podataka o API vezi za Cloudant® NoSQL DB i streamove događaja.

Korak 4: Analizirajte svoje IoT podatke

Vaši IoT podaci sami po sebi obično nisu korisni. Analiza podataka donosi vrijednost vašim IoT rješenjima. Watson IoT platforma dolazi s unaprijed instaliranim alatima za analizu u stvarnom vremenu i povijesnim analizama pomoću kojih možete dodati vrijednost svojim podacima.

- **Monitoring dashboards.** Pregledajte kurirane podatke poslovnih korisnika za svoje entitete. Prilagođene nadzorne ploče mogu sadržavati kurirane IoT podatke s vaših uređaja, kao i uvezene vanjske podatke. Nadzorne ploče napajaju se iz podatkovnog jezera.
- **Real-time analytics.** U usluzi Platform koristite ugrađena pravila za upravljanje podacima da biste dodali uvjete svojim IoT podacima i vidjeli upozorenja i izvršili radnje kada su zadovoljeni pragovi i drugi uvjeti.
- **Historical data analytics.** Da bi nadopunila analitiku u stvarnom vremenu temeljenu na pravilima, Watson IoT platforma nudi integriranu analitiku kao i analitičke alate koji su uključeni u komponentu Db2 Warehouse on Cloud.

Korak 5: Izradite servisnu app

Nakon postavljanja infrastrukture, IoT podaci teku, sve su komponente povezane i pokreće se osnovna analitika, sada ste spremni iskoristiti punu snagu Watson IoT platforme izgradnjom vlastitog aplikacijskog rješenja.

Korak 6: Upotrijebite Object Storage za pristup svojim dugoročnim IoT podacima

Kao dio procesa životnog ciklusa podataka, IBM® Cloud Object Storage duži vremenski period pohranjuje kompletan niz povijesnih podataka. Na primjer. povijesne podatke možete zadržati u svrhu revizije ili ih koristiti za dugoročnu analitiku.

Dugoročne podatke možete preuzeti iz Object Storage:

- Uvezite JSON objekt u Db2 Warehouse na Cloud za daljnju analitiku.
- Uvezite JSON objekt u svoj vlastiti alat za analitiku.

Smjernice za izradu sobnog temperaturnog senzora

Na ovom mjestu za vas smo pripremili kratki vodić za obavljanje nekih osnovnih zadataka za pokretanje Watson IoT platforme.

Prvi zadaci koje trebate izvršiti kada počnete koristiti proizvod uključuju unošenje podataka u podatkovno jezero, primjenu izračuna na podatke i prikaz rezultata na nadzornoj ploči.

U vodiču simulirate sobni senzor u konferencijskoj sobi za mjerenje popunjenosti sobe i sobne temperature. Zauzetost sobe daje se kao postotak kapaciteta sobe, a temperatura se mjeri u Celzija. Konfigurirate nadzornu ploču za praćenje razina zauzetosti i odstupanja u vrijednostima temperature tijekom razdoblja od 24 sata.

Korak 1: Simulirajte podatke o entitetu

1. Prijavite se u Maximo Application Suite.
2. Odaberite Maximo Asset Monitor iz navigatora aplikacije.
3. Na bočnom izborniku odaberite „**Connect**“.
4. Na pločici Poveži kliknite „**Connect**“.

   Nadzorna ploča usluge platforme otvara se na kartici „**Browse**“ na stranici Uređaji.
5. Na nadzornoj ploči usluge platforme kliknite poruku „**0 Simulations running**“.

   Savjet: Ako simulator uređaja nije dostupan, omogućite simulaciju uređaja za svoj korisnički ID.

   - U glavnom navigacijskom oknu odaberite **Settings**.
   - U odjeljku Podaci i uređaji aktivirajte simulator uređaja.
6. U prozoru za konfiguraciju simulacija koji se otvori kliknite **Create Simulation**.
7. Stvorite vrstu uređaja **Room_sensor**.

   Ako ime već postoji, dodijelite jedinstveno ime i promijenite sve reference na **Room_sensor** na to ime.
8. Unesite **room_status** za vrstu događaja.
9. Postavite opterećenje događaja na:

```
{
  "zauzetost": slučajno (0, 100),
  "temp": slučajno (15, 35)
```

```
} `
```

Važno: U podatkovnom jezeru imena stavki podataka imaju prefiks s tekstom `room-status`.

10. Omogućite **Save events as historical data** kako biste učinili dostupnim simulirano stanje uređaja putem automatski stvorenog logičkog sučelja i pohranili podatke uređaja za kasniji pristup.
11. Kliknite **Save** da biste stvorili vrstu uređaja.
12. Kliknite **Screate Simulated Device** da biste stvorili jedan uređaj i započeli slanje podataka.

    Napomena: Simulirani nazivi uređaja izvedeni su izravno iz vrste uređaja, na primjer, Room_sensor_1.
13. Provjerite povećava li se broj poslanih događaja.
14. Provjerite šalju li se događaji na uređaju.
    - Odaberite karticu **Browse**.
    - U polje za pretraživanje unesite naziv vrste uređaja.
    - Odaberite jedan od svojih uređaja.
    - Otvorite karticu **State**.
    - Kao opciju interfejsa odaberite **Raw Data**.
    - Prikazuju se simulirane vrijednosti.

      Važno: Simulator uređaja radi dok je aktivna vaša sesija nadzorne ploče usluge platforme. Simulator uređaja ne šalje podatke ako ste odjavljeni sa sesije.

Korak 2: Istražite mjerne podatke entiteta

Vrste vaših uređaja automatski generiraju vrste entiteta i pohranjuju odgovarajuće podatke o entitetima u podatkovno jezero.

Važno: Podatkovno jezero sadrži povijesne podatke i popunjava se dok vaši uređaji daju podatke. Vremenski odmak nastaje između prvog povezivanja uređaja i početka prikazivanja podataka.

1. Na korisničkom sučelju odaberite **Monitor**.
2. Odaberite vrstu entiteta `Room_Sensor_1`.

3. Odaberite karticu **Data** da biste pogledali podatke koji su pohranjeni u podatkovnom jezeru.

   Dvije podatkovne točke odgovaraju korisnom opterećenju uređaja koje je izravno mapirano logičkim sučeljem i koje uključuje sljedeća svojstva uređaja:

   - `occupancy` - cijeli broj koji predstavlja postotak popunjenosti u rasponu od 0-100.
   - `temp` - Cijela temperatura u rasponu od 15-35 C.

4. Odaberite stavku privremenih podataka iz stupca Podaci za prikaz privremenih ulaznih podataka za uređaj.

Podaci vašeg uređaja sada ulaze u podatkovno jezero, a vi dodajete izračun pomoću ugrađene funkcije.

Korak 3: dodajte izračune

Ulaznim podacima dodajte izračune upotrebe. Izračunajte standardno odstupanje podataka o temperaturi.

1. U korisničkom sučelju odaberite **Monitor**.
2. Odaberite vrstu entiteta `Room_Sensor_1`.
3. Odaberite karticu **Data** da biste pogledali podatke koji su pohranjeni u data lake.
4. Kliknite +
5. Pregledajte katalog funkcija i odaberite funkciju **StandardDeviation**.
6. Odaberite mjernu vrijednost **temp** kao izvor i imenujte izračunatu mjernu vrijednost `temp_sigma`.
7. Odaberite granularnost koja će se koristiti za izračun, na primjer **Daily**.
8. Pričekajte nekoliko minuta da se pokrenu planirani izračuni, a zatim se vratite na karticu **Data** i pogledajte svoju novu izračunatu mjernu vrijednost.

Korak 4: dodajte nadzornu ploču instance

Stvorite JSON datoteku sa sljedećom konfiguracijom nadzorne ploče. Nadzorna ploča uključuje dvije linijske grafičke kartice. Prva karta prikazuje zauzetost entiteta u posljednja 24 sata. Druga karta prikazuje srednju i maksimalnu temperaturu tijekom posljednja 24 sata.

Napomena: Nadzorna ploča stvara srednju i maksimalnu skupnu funkciju.

U primjeru JSON, unos `dataSource / attributes / attribute` odgovara stavci podataka `room_status_occupancy` i stavci podataka `temp_sigma`.

```
{
    "title": "Room Sensor Graph",
    "cards": [{
            "id": "room_sensor_occupancy",
            "size": "LARGE",
            "title": "Room occupancy - input values",
            "type": "TIMESERIES",
            "content": {
                "series": [{
                        "dataSourceId": "occupancyID",
                        "label": "Occupancy "
                    }
                ],
                "unit": "%"
            },
            "dataSource": {
                "attributes": [{
                        "attribute": "room_status_occupancy",
                        "id": "occupancy_ID"
                    }
                ],
                "range": {
                    "count": -24,
                    "interval": "hour"
                }
            }
        },
        {
            "id": "room_sensor_temp",
            "size": "LARGE",
            "title": "Temperature stanard deviation data mean vs
max",
            "type": "TIMESERIES",
            "content": {
                "series": [{
                    "dataSourceId": "temp_sigma_ID",
                    "label": "Temp - standard deviation"
                }]
            },
            "dataSource": {
                "attributes": [{
                    "attribute": "temp_sigma",
                    "id": "temp_sigma_ID"
                }],
                "range": {
                    "count": -24,
                    "interval": "hour"
                }
            }
        }
    ]
}
```

1. Na bočnom izborniku odaberite **Monitor**.
2. Odaberite vrstu entiteta `Room_Sensor`.
3. Kliknite ikonu Konfiguracija, a zatim odaberite **Manage instance dashboard**.
4. Prenesite datoteku za konfiguraciju nadzorne ploče JSON.
5. Provjerite izgleda li nadzorna ploča prema očekivanjima, a zatim kliknite **Save**.

Korak 5: Pogledajte mjerne podatke za svoje entitete

Vizualizirajte podatke kao kartice pomoću značajke nadzorne ploče.

1. Na kartici **Entitis** odaberite vrstu entiteta `Room_Sensor`.
2. Pod nadzornom pločom Instance odaberite entitet `Room_Sensor_1` da biste otvorili nadzornu ploču instance.
3. Provjerite možete li s ove nadzorne ploče nadzirati podatke o zauzetosti.
4. Promijenite vremenski raspon tako da se prikazuju podaci o posljednjih 7 dana zauzetosti.
5. Promijenite vrijeme sidrenja na nadzornoj ploči na jučerašnje i pogledajte kako utječe na vremenski raspon na svim karticama.

Zadaci za brzi početak

Zadaci brzog pokretanja pokrivaju neke osnovne zadatke koji započinju s Maximo Asset Monitorom.

Ako tek započinjete s proizvodom, korisno je koračati kroz ove zadatke u nizu, jer se svaki zadatak nadovezuje na prethodne.

- Spojite uređaj
- Stvorite logično sučelje
- Istražite podatke o entitetima
- Dodajte funkciju
- Pregledajte mjerne podatke na nadzornoj ploči

1. Spajanje uređaja

Da biste vidjeli kako se podaci vašeg uređaja prelijevaju u uslugu platforme, prvo morate povezati uređaj i poslati neke događaje.

Korak 1: dodajte vrstu uređaja

Da biste mogli registrirati i povezati svoje uređaje s uslugom platforme, morate stvoriti vrstu uređaja.

1. Na korisničkom sučelju usluge Platform odaberite: **Device> Device Types**, a zatim kliknite **Add Device Type**.
2. Dodijelite ime vrsti uređaja i kliknite **Next**.
3. (Izborno) Dodijelite dimenzije ili meta podatke vrsti uređaja. Zatim se svim dimenzijama dodanim vrstama uređaja zadaju ove dimenzije.

   Primjer:

```
{
    "country": "Njemačka",
    "poredak": 2,
    "city": "Berlin"
}
```

4. Pritisnite **Finish**.

Korak 2: Dodajte uređaj

Kada dodate uređaj na uslugu platforme, kreirate virtualni prikaz tog uređaja. Virtualni prikaz ima jedinstveni ID uređaja i jedinstveni API pristupni token.

Napomena: U beta okruženju Maximo Asset Monitor možete dodati uređaj s kartice **Connect**. Kliknite **Add a device** i slijedite čarobnjaka slijedeći sljedeće korake kao smjernice.

1. Odaberite: **Device > Browse**, a zatim kliknite **Add Device**. Napomena: Svaki uređaj pripada tipu uređaja.
2. Odaberite vrstu uređaja. Ako ne postoji vrsta uređaja, prvo ga morate stvoriti.
3. Uređaju dodijelite ID uređaja i kliknite **Next**.
4. (Izborno) Ažuriranje vrijednosti dimenzija ili meta podataka. Po želji dodajte novu dimenziju uređaja.

   Primjer:

```
{
    "country": "Njemačka",
    "poredak": 2,
    "city": "Frankfurt"
}
```

5. Uređaju dodijelite token za provjeru autentičnosti. Ako ga ne dodijelite, token se automatski generira za vas.
6. Zapišite jedinstveni ID uređaja i token koji ste konfigurirali za uređaj. Ovi se parametri koriste za upućivanje na vaš uređaj.
7. Pritisnite **Finish**.

Korak 3: Pošaljite podatke

Da biste vidjeli kako se podaci vašeg uređaja prelijevaju u uslugu platforme, prvo morate povezati svoj uređaj i poslati neke događaje.

1. Konfigurirajte svoj uređaj za slanje MQTT poruka Platform Serviceu.

   Za povezivanje uređaja upotrijebite sljedeće podatke:

   - Usmjerite uređaj na sljedeći URI:

     `https: // <orgId> .messaging.internetofthings.ibmcloud.com`

   - Za provjeru autentičnosti pogledajte Basic Auth s use-token-auth kao korisničkim imenom i tokenom koji ste stekli kada ste uređaj registrirali kao lozinku.
   - Koristite ovu krajnju točku REST API-ja:

   `POST / device / types / {typeId} / devices / {deviceId} / events / {eventName}`

Upotrijebite `typeId` i deviceId koje ste prethodno definirali.

Na primjer: `POST`

`/ device / types / Room_sensor / devices / Room_sensor_1 / events / room_status`

2. Konfigurirajte korisni teret tako da uključuje IoT podatke koje želite uključiti.

   Na primjer, za slanje poruke o statusu i očitanja trenutne temperature možete upotrijebiti sljedeće korisno opterećenje:

```
{"occupancy": 25, "temp": 22}
```

3. Pošaljite poruku i korisničkim sučeljem usluge Platform provjerite jesu li primljeni podaci uređaja:
   - Prijavite se u Maximo Application Suite.
   - Iz navigatora aplikacije odaberite Maximo Asset Monitor.
   - Na bočnom izborniku odaberite **Connect**.
   - Na pločici Povezivanje kliknite **Connect**. Korisničko sučelje usluge Platform otvara se na kartici **Browse** na stranici **Devices**.
   - Odaberite **Devices > Browse**.
   - S popisa registriranih uređaja odaberite svoj uređaj, a zatim odaberite karticu **Recent events**.
   - Provjerite slijede li događaji na vašem uređaju kako se očekivalo.

     Prethodni primjer korisnog tereta rezultira sljedećim statusom događaja:

     ```
     room_status {"zauzetost": 25, "temp": 22} json a few seconds ago
     ```

   - Ako nisu dostupni nedavni događaji, odaberite karticu **State** da biste vidjeli zadnji isporučeni događaj za uređaj.

2. Kreiranje logičkog interfejsa

Koristite logički interfejs za stvaranje jedinstvenog logičkog prikaza podataka vašeg povezanog uređaja koji vaše aplikacije mogu lako unijeti. Svaka vrsta uređaja može imati više logičkih interfejsa.

Vi možete stvoriti logički interfejs koji mapira svojstva dolaznog uređaja izravno u logički prikaz za pohranu podataka uređaja u podatkovno jezero.

1. Na korisničkom sučelju usluge Platform odaberite: **Devices > Devices Types**.
2. Odaberite vrstu uređaja za koji želite stvoriti sučelje i kliknite **Interface**.
3. Kliknite **Advanced Flow**, a zatim **Create Physical Interface**.
4. Dodijelite naziv sučelju ili prihvatite zadani naziv i kliknite Next.
5. Definirajte fizički interfejs:
   1. Kliknite **Create event type**.
   2. Kliknite **manually** u polje za tekst.

3. Dodijelite naziv i ID tipa događaja, na primjer, `room_status`.
4. Kliknite **Add another property** da biste dodali svojstva.
   - Dodajte sve značajke koje uključujete u korisni teret svog uređaja.
   - Dodijelite vrstu podataka i navedite je li svojstvo obvezno.
   - Kliknite Done.

6. Definirajte logički interfejs.
   1. Kliknite **Create Logical Interface**.
   2. Dodijelite naziv interfesu i kliknite **Next**.
   3. Na stranici `Model State` kliknite **Add Property**.
   4. Odaberite svojstvo i kliknite **Save**.
   5. Ponovite za svako svojstvo u korisnom opterećenju vašeg događaja.
   6. Kliknite **Next**.
7. Na kartici `Notifications tab` postavite kriterije obavijesti na **All events** i kliknite **Apply**.
8. Kliknite **Done**.
9. Kliknite **Activate** i potvrdite da želite aktivirati vrstu uređaja.
10. Kliknite **Done**.
11. Pronađite svoj uređaj. Na kartici `Browse tab` potražite svoj uređaj.
12. Odaberite karticu **State**, a zatim odaberite sučelje koje ste stvorili.
13. Provjerite jesu li prikazani događaji koje vaš uređaj podnosi usluzi platforme.

Sada se možete pretplatiti ili zatražiti podatke o trenutnom stanju za svoje uređaje s logičkog interfejsa.

Upotrijebite sljedeći poziv HTTP REST API da biste dobili trenutno stanje logičkog sučelja:

```
GET
/ device / types / {typeId} / devices / {deviceId} / state / {logicInterfaceId}
```

Gdje je `{logicInterfaceId}` ID vašeg logičkog sučelja

Da biste dobili ID svog logičkog sučelja:

1. Na kartici **Device Type** potražite vrstu uređaja.
2. Odaberite **Interface**.
3. Kliknite **View**
4. Pronađite svoj logički ID sučelja na kartici Identity i kopirajte ga.

Također možete prilagoditi sučelje, na primjer, za mapiranje različitih dolaznih svojstava u isto svojstvo logičkog sučelja, pretvaranje očitanja temperature između temperaturnih ljestvica ili mapiranje svojstava u ljudsko čitljiva imena kako bi ih učinili potrošnijima. Da biste započeli s prilagodbom vašeg sučelja, odaberite vezu **Use Advanced Interface Creator** na kartici **Interface**.

3. Istražite podatke o entitetima

Kad podaci s vaših uređaja uđu, oni se prikazuju kao mjerni podaci u prikazu entiteta korisničkog interfejsa.

Vrste vaših uređaja automatski generiraju tipove entiteta i pohranjuju odgovarajuće podatke o entitetima u podatkovno jezero.

Važno: Podatkovno jezero sadrži povijesne podatke i popunjava se dok vaši uređaji doprinose podacima. Vremenski odmak nastaje između prvog povezivanja uređaja i početka prikazivanja podataka.

Istražite podatke uređaja koji su pohranjeni u podatkovnom jezeru:

1. Na bočnom izborniku odaberite **Monitor**.
2. Odaberite vrstu entiteta koja odgovara vrsti uređaja vašeg uređaja.
3. Odaberite karticu **Data** da biste pogledali podatke koji su pohranjeni u podatkovnom jezeru.
4. Odaberite svojstvo iz stupca `Data` da biste pregledali mjerne podatke podataka za uređaj.

Podaci vašeg uređaja sada slijevaju u podatkovno jezero i možete započeti obradu podataka u izračunate mjerne podatke dodavanjem funkcije.

4. Dodavanje funkcije

Obradite ulazne mjerne podatke entiteta stvaranjem izračunanih mjernih podataka pomoću funkcija.

To možete uraditi na slijedeći način:

1. Na bočnom izborniku odaberite **Monitor**.
2. Odaberite vrstu entiteta koja odgovara vrsti uređaja za vaš registrirani uređaj.
3. Odaberite karticu **Data** da biste pogledali podatke pohranjene u podatkovnom jezeru.
4. Kliknite +
5. Pregledajte katalog funkcija i odaberite funkciju koju želite koristiti za izračunavanje novih podataka. Možete, na primjer, možeze upotrijebiti **StandardDeviation** za izračunavanje standardnog odstupanja u skupu podataka za podatkovnu stavku.
6. Odaberite mjernu vrijednost izvora i dajte izračunu naziv.
7. Odaberite granularnost koja će se koristiti za izračun, na primjer **Daily**.
8. Pričekajte nekoliko minuta da se pokrenu planirani izračuni, a zatim se vratite na karticu `Data tab` i pogledajte svoju novu izračunatu mjernu vrijednost.

4. Pregled metrike u Dashboard-u

Vizualizirajte metriku entiteta u nadgledanju nadzornih ploča kako biste dobili pregled podataka.

Podatke možete vizualizirati i kao kartice pomoću nadzorne ploče na slijedeći način:

1. Na bočnom izborniku odaberite **Monitor**.
2. Odaberite vrstu entiteta za koji želite dodati nadzornu ploču.
3. Kliknite ikonu , a zatim odaberite **Manage instance dashboard**.
4. Prenesite lokalnu konfiguracijsku datoteku JSON nadzorne ploče.
5. Provjerite izgleda li nadzorna ploča prema očekivanjima, a zatim kliknite **Save**.

Možda ćete morati pričekati nekoliko minuta prije nego što se podaci pojave.

Primjer JSON konfiguracije nadzorne ploče dat je na slijedećem prikazu.

Napomena: U ovom primjeru zamijenite `<metric>` imenom stavke podataka iz vašeg entity type.

```
{
    "title": "Sample instance dashboard",
    "cards": [{
        "content": {
            "series": [{
                "dataSourceId": "<metric>_ID",
                "label": "<metric>"
            }]
        },
        "dataSource": {
            "attributes": [{
                "attribute": "<metric>",
                "id": "<metric>_ID"
            }],
            "range": {
                "count": -24,
                "interval": "hour"
            }
        },
        "id": "line_graph_card_metric",
        "size": "LARGE",
        "title": "Metric for the lastt 24 hours",
        "type": "TIMESERIES"
    }]
}
```

Korištenje Watson IoT Platform Dashboard

Nadzornu ploču Watson IoT Platform možete koristiti za pristup pojedinačnim uslugama koje čine ponudu, praćenje korištenja i upravljanje pristupom nadzornoj ploči.

Nadzorna ploča Watson IoT Platform sastoji se od nekoliko odjeljaka koji vam omogućuju upravljanje različitim aspektima vašeg okruženja Watson IoT Platform:

- **Nadzorna ploča**

Omogućite brz pristup nadzornim pločama za praćenje vrsta entiteta u usluzi Analytics.

- **Monitor**

Pregledajte povezane vrste entiteta i istražite mjerne podatke i dimenzije svojih entiteta u usluzi Analytics. Postavite nadzorne ploče za nadzor kako bi saželi i vizualizirali ključne podatke o entitetima za poslovne korisnike.

- **Povezivanje**

Uspostavite veze za izvođenje podataka sa svojih uređaja u usluzi Platform i stvorite vrste entiteta s kojima možete raditi.

- **Usluge**

Pregledajte i pristupite uslugama koje su uključene u vašu ponudu platforme Watson IoT. Pogledajte informacije o planu i statistiku korištenja usluga.

- **Korisnici**

Dodajte korisnike u komponentu Monitor Maximo Asset Monitor i upravljajte onim što imaju pristup. Važno:Korisnička uloga daje pristup samo korisničkom sučelju. Za ostale usluge koje su uključene u vaš proizvod, na korisničkom sučelju kliknite **View Details** za prikaz `credentials` i pristup odgovarajućoj nadzornoj ploči usluge.

- **Najave**

Pristupite i pretplatite se na najave relevantne za vaše rješenje, lokaciju usluge ili određenu instancu usluge.

Da biste pristupili nadzornoj ploči Watson IoT Platform, upotrijebite URL i podatke za prijavu koji se nalaze u pozdravnom pismu vaše IBM® Watson ™ IoT Platforme.

Važno: Da biste pristupili nadzornoj ploči Watson IoT Platform, vaša adresa e-pošte povezana s IBMid mora se dodati kao korisnik nadzorne ploče Watson IoT Platform

Monitor

Upotrijebite odjeljak **Monitor** za izradu izračunatih mjernih podataka i dimenzija za uslugu **Analytics services** vašeg entiteta. Konfigurirajte neke prilagođene nadzorne ploče za nadzor za svoje vrste entiteta. Nadzorne ploče mogu sadržavati podatke o trenutnom stanju entiteta i izračunate mjerne podatke (potreban je dodatak usluge Analytics).

Za više informacija o stvaranju izračuna, pogledajte temu Usluga Analytics (dodavanje). Za više informacija o prilagođenim nadzornim pločama pogledajte temu Nadzor nadzornih ploča.

Povezivanje

Upotrijebite odjeljak **Connect** konfiguriranje izvora podataka za vaše okruženje Watson IoT Platform.

Da biste se povezali s IoT uređajima, kliknite **Connect** i nastavite postupak povezivanja pomoću nadzorne ploče Platform Service.

Usluge

Pratite razinu upotrebe na uslugama koje su uključene u vaš plan i pogledajte detalje o tim uslugama.

Mogu se prikazati sljedeće usluge i njihovi odgovarajući podaci o korištenju:

- Platform Service
- IBM® IoT usluga registracije
- Cloudant NoSQL DB
- IBM® Db2® Warehouse on Cloud
- Baze podataka za PostgreSQL
- IBM® Cloud Object Storage
- IBM Cloud App ID
- IBM® Event Streams for IBM Cloud
- IBM® Secure Gateway for IBM Cloud
- IBM® Watson ™ IoT Platform on Blockchain

Pristup nadzornim pločama usluge

Sljedeće usluge imaju vlastite nadzorne ploče:

- Platform Service
- Db2® Warehouse on Cloud

Da biste pristupili pojedinačnoj nadzornoj ploči za svaku uslugu:

Na nadzornoj ploči Watson IoT Platform kliknite **View Details** za uslužnu nadzornu ploču kojoj želite pristupiti.

Kliknite **Launch** da biste otvorili nadzornu ploču, a zatim unesite vjerodajnice za prijavu.

- Db2® Warehouse on Cloud

  Prijavite se s vjerodajnicama za uslugu s nadzorne ploče Watson IoT Platform.

- Platform Service

  1. Kliknite **Sign In** na odredišnoj stranici nadzorne ploče usluge platforme, a zatim se prijavite s IBMid-om koji je naveden u vašem pozdravnom pismu ili s IBMid-om kojem ste odobrili pristup. Za više informacija pogledajte Upravljanje korisničkim pristupom u dokumentaciji usluge platforme.

2. Ako je vaš IBMid član više od jedne organizacije za pružanje usluga na platformi, odaberite Watson IoT Platform organizaciju s izbornika Moje organizacije

   Savjet: Šestslovni ID organizacije uključen je na stranicu vjerodajnica.

Pristup uslužnim API

Da biste pronašli vjerodajnice za API za svaku uslugu:

1. Na nadzornoj ploči Watson IoT Platform kliknite View Details za uslugu.
2. Kopirajte vjerodajnice za API.

   Na primjer, za pristupnu kopiju API-ja za uslugu platforme: OrgId, API ključ, API token i URL hosta.

Praćenje upotrebe

Vaša pretplata na uslugu uključuje dodijeljeno korištenje za svaku uslugu. Upotreba može biti u obliku broja obrađenih megabajta, broja povezanih uređaja (usluga platforme) i broja spremljenih megabajta (Cloudant NoSQL DB, Db2® Warehouse on Cloud).

Uz ovu dodjelu, možete dodati i međuspremnik za neraspoređenu upotrebu u obliku ugovorenih jedinica kapaciteta. Na primjer, možete koristiti ugovorene jedinice kapaciteta ako znate da će vaša potrošnja za jedan ili više mjernih podataka premašiti vaš plan, ali ne želite nadograditi plan. Za više informacija ili prilagodbu pretplate kontaktirajte imenovanog administratora.

Definicija jedinice kapaciteta razlikuje se ovisno o metričkim podacima i kategoriji pretplate na uslugu. Na primjer, jedinica kapaciteta za metriku Broj uređaja može biti 60 uređaja, a jedinica kapaciteta za metriku Razmijenjeni podaci može biti 800 MB.

Podaci o upotrebi

Kartica **Services** na nadzornoj ploči Watson IoT Platform prikazuje pregled upotrebe vašeg uređaja, kao i sljedeće informacije o upotrebi za svaku uslugu:

- Pretplaćeni - mjesečna dodjela po vašem planu.
- Potrošeno - upotreba za tekući mjesec.

- Planiranje prekomjerne potrošnje - bilo koji višak potrošnje, u jedinicama kapaciteta, za tekući mjesec.Plavi pokazatelji prekomjerne potrošnje pokazuju prekomjerne količine koje pokrivaju jedinice ugovorenog kapaciteta. Crveni indikatori prekomjerne potrošnje pokazuju višak koji premašuje jedinice ugovorenog kapaciteta. Dodatni iznos bit će vam naplaćen.

Pristup Starter app (Početna aplikacija)

Početna aplikacija dostupna je za neproizvodna okruženja i može joj se pristupiti iz odjeljka `Sample application` na nadzornoj ploči platforme Watson IoT.

S nadzorne p loče možete izvršiti sljedeće zadatke:

- Kliknite vezu **Route** da biste otišli na nadzornu ploču aplikacije.
- Kliknite vezu **Git** pod Izvorni kôd da biste pristupili uzorcima početnog koda i predlošcima.
- Kliknite vezu **Logs** da biste pristupili zapisnicima početne aplikacije.

  Pregledajte najnovije zapisnike ili kliknite **Copy to clipboard** ikonu za lijepljenje zapisnika (eng. logs) u vašu omiljenu proračunsku tablicu ili alat za uređivanje.

Korisnici

Kartica **Users** pruža alate koji su vam potrebni za dodavanje, brisanje i upravljanje vašim nadzornim pločama Watson IoT Platform dodjeljivanjem korisničkih uloga nadzorne ploče IBMid.

Važno: Uloga korisnika nadzorne ploče omogućuje samo pristup nadzornoj ploči Watson IoT Platform. Za ostale usluge koje su uključene u vaš proizvod, na nadzornoj ploči platforme Watson IoT Platforma kliknite **View Details** za prikaz vjerodajnica i pristup odgovarajućoj nadzornoj ploči usluge.

Uslužne najave

Povremeno se objavljuju najave relevantne za vaše rješenje, lokaciju usluge ili određenu instancu usluge. Možete im pristupiti iz izbornika **Annoncements menu**. Brojač pokazuje broj nedavno objavljenih novih najava.

Savjet: Najave se možete pretplatiti i putem RSS feeda ili e-poštom. Kliknite odgovarajuću ikonu u izborniku Obavijesti, da biste vidjeli popis adresa RSS feedova ili konfigurirali pretplate na e-poštu za sve ili podskup održavanja, nezgoda, sigurnosti i općih najava.

Spajanje sa uređajima

Kreiranje logičkog interfesa

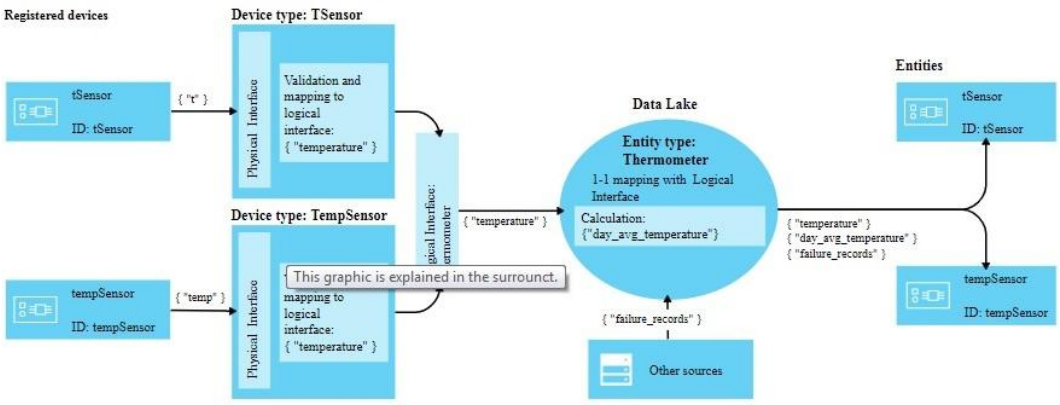
Prije nego što počnete primati podatke sa svojih IoT uređaja, morate ih povezati s uslugom platforme. Morate stvoriti i logički interfejs koja se u usluzi Analytics pretvaraju u vrste entiteta.

Usluga Analytics koristi tipove entiteta za grupiranje dolaznih mjernih podataka, dimenzija i događaja. Da biste stvorili tipove entiteta, prvo morate stvoriti i aktivirati logički interfejs za svoje tipove podataka. Svako logičko sučelje stvara novi tip logičkog entiteta i to logičko sučelje možete ponovo koristiti za više vrsta uređaja.

Logičko sučelje koristi se za definiranje normaliziranog pogleda u stanje uređaja u usluzi platforme.

Sljedeći dijagram ilustrira kako se logički interfejs može koristiti za pretvaranje više uređaja u jedan tip entiteta:

Prikaz: Kreiranje logičkog interfejsa za spajanje uređaja



O uređajima

Uređaji su stvari koje direktno ili indirektno šalju podatke Platform Serviceu i koje reagiraju na naredbe poslane s usluge.

Pomoću uređaja izvršite sljedeće zadatke:

- Šaljete događaje.
- Primate naredbe.

Uređaji objavljuju podatke usluzi platforme pomoću događaja (eng. events). Uređaj kontrolira sadržaj događaja i dodjeljuje naziv svakom događaju koji se pošalje. Kada usluga platforme primi događaj uređaja, vjerodajnice veze na koju je događaj primljen koriste se za utvrđivanje s kojeg je uređaja događaj poslan. Ova arhitektura sprečava uređaj da se lažno predstavlja kao drugi.

- Za informacije o službenim SDK-ovima koji podržavaju razvoj uređaja, pogledajte SDK za uslugu platforme.
- Referentni uzorci klijenta uređaja dostupni su i za razne jezike. Koristite ih kao početnu točku za pokretanje vašeg projekta Usluga platforme.

Registracija uređaja

Uređaj mora biti registriran u organizaciji prije nego što se može povezati s uslugom platforme. Registrirani uređaji identificiraju se na usluzi Platform s jedinstvenim identifikatorom uređaja koji se sastoji od četiri dijela:

- ID klase `(classId)`.

  Ovo identificira uređaj kao standardni uređaj kada je postavljen na d.

- Organization ID `(orgId)`.

  Ovo je globalno jedinstveni identifikator za vašu instancu, dodijeljen prilikom prve registracije na IBM Watson IoT Platform.

- Type ID (`typeId`).

  Ovo je ID vrste uređaja, jedinstven u vašoj organizaciji. Smatrajte ovo analognim broju modela.

- Device ID (`deviceId`).

  Ovo je ID uređaja. Jedinstven je samo u uređajima određene vrste. Smatrajte ovo analognim serijskom broju.

Savjet: Uređaji u usluzi Platform namijenjeni su zrcaljenju fizičke implementacije hardvera koji generira IoT podatke, bez obzira na to povezuje li se taj hardver izravno s internetom ili ne. Primjer: Ako rasporedite šest dijelova hardvera, svaki s odvojenim atributima kao što su firmware i softver, trebali biste izbjeći napast da ih spojite u "apstraktni uređaj" koji predstavlja svih šest kada registrirate svoj fizički model uređaja. Spajanje ovakvih uređaja otežava upotrebu naprednih mogućnosti usluge platforme za upravljanje uređajima i podacima.

Autentifikacija uređaja

Usluga platforme podržava dvije metode provjere autentičnosti:

- Default: provjera autentičnosti na temelju tokena.

  Pri registraciji uređaja, po želji možete dati token za provjeru autentičnosti koji uređaj mora koristiti ili možete dopustiti da ga usluga generira za vas.

- Provjera autentičnosti klijentskog certifikata.

Povezivanje uređaja

Kad god je to tehnički moguće, MQTT je preferirani način povezivanja uređaja s uslugom platforme. Povezivost uređaja preko MQTT-a u potpunosti je pokrivena MQTT povezivošću za uređaje.

U slučajevima kada MQTT nije opcija za povezivanje uređaja, možete koristiti API za razmjenu poruka HTTP za slanje događaja i primanje naredbi bez povezivanja uređaja s uslugom platforme.

Komuniciranje sa uređajima (MQTT)

Primarni protokol koji uređaji i aplikacije koriste za komunikaciju s uslugom platforme je MQTT.

Usluga brzog pokretanja

Usluga Quickstart najbrža je razina usluge. Ne nudi potvrdu primitka i ne podržava razine kvalitete usluge MQTT (QoS) veće od nule. Kada se povežete s uslugom Quickstart, provjera autentičnosti ili registracija nije potrebna, a orgId mora biti postavljen na `quickstart`.

Ako pišete kôd uređaja za upotrebu s Quickstartom, imajte na umu da sljedeće značajke usluge Platform Service nisu podržane u načinu Quickstart:

- Subscribing to commands
- Device Management Protocol
- Clean or durable sessions

Važno: Poruke koje se šalju s uređaja brzinom većom od jedne u sekundi mogu se odbaciti.

MQTT provjera autentičnosti

Za uređaje, Platform Service koristi provjeru autentičnosti na temelju MQTT tokena.

Da biste omogućili MQTT provjeru autentičnosti, pošaljite korisničko ime i lozinku prilikom uspostavljanja MQTT veze.

- **Korisničko ime**

Korisničko ime jednaka je vrijednost za sve uređaje: **use-token-auth**. Ova vrijednost uzrokuje da Platform Service koristi token za provjeru autentičnosti uređaja, koji je naveden kao lozinka.

- **Password**

Lozinka za svaki uređaj je jedinstveni token za provjeru autentičnosti koji je generiran kad je uređaj registriran u Platform Service.

- **Client ID**

ID MQTT klijenta je u formatu `d: orgId: deviceType: deviceId`.

Objavljivanje događaja

Uređaji objavljuju teme događaja u sljedećem formatu:

```
iot-2 / evt / event_id / fmt / format_string
```

Gdje

- **event_id** je ID događaja, na primjer status. ID događaja može biti bilo koji niz koji vrijedi u MQTT-u. Kada prima ove poruke događaja, aplikacija za pretplatu može koristiti zamjenski znak za primanje događaja s bilo kojim ID-om ili se pretplatiti s id-om događaja koji se podudara s id-om događaja koji je izdavač koristio.

- **format_string** je niz koji definira vrstu sadržaja korisnog tereta poruke tako da primatelj poruke može odrediti način raščlanjivanja sadržaja. Uobičajene vrijednosti vrste sadržaja uključuju, ali nisu ograničene na "json", "xml", "txt" i "csv". Vrijednost može biti bilo koji niz koji vrijedi u MQTT-u.

Važno: Korisna težina poruke ograničen je na najviše 131072 bajta. Poruke veće od ovog ograničenja odbijaju se.

Organizacije za platforme nisu ovlaštene objavljivati zadržane MQTT poruke. Ako uređaj pošalje zadržanu poruku, usluga usluge platforme poništava zastavu zadržane poruke kada je postavljena na true i obrađuje poruku kao da je zastavica zadržane poruke postavljena na false.

Pretplata na naredbe (eng. Subscribing to commands)

Uređaji se mogu pretplatiti na teme naredbi u sljedećem formatu:

```
iot-2 / cmd / command_id / fmt / format_string
```

Gdje

- **command_id** je ID naredbe, na primjer, update. ID naredbe može biti bilo koji niz koji vrijedi u MQTT protokolu. Kada prima ove poruke naredbi, pretplatnički uređaj može koristiti zamjenski znak za primanje naredbi s bilo kojim ID-om ili se pretplatiti s command_id koji odgovara command_id koji je izdavač koristio.
- **format_string** je niz koji definira vrstu sadržaja naredbe korisnog tereta tako da primatelj naredbe može odrediti način raščlanjivanja sadržaja. Uobičajene vrijednosti vrste sadržaja uključuju, ali nisu ograničene na "json", "xml", "txt" i "csv". Vrijednost može biti bilo koji niz koji vrijedi u MQTT-u.

Uređaji se ne mogu pretplatiti na događaje s drugih uređaja. Uređaj prima naredbe koje se objavljuju samo na njegovom vlastitom uređaju.

Upravljanje uređajima

Podrška za upravljanje životnim ciklusom uređaja nije obavezna. Protokol za upravljanje uređajima koristi istu MQTT vezu koju vaš uređaj već koristi za događaje i kontrolu naredbi.

Upravljani uređaji mogu objavljivati poruke s razinom kvalitete usluge (QoS) od 0, 1 ili 2.

Poruke koje imaju razinu QoS-a 0 mogu se odbaciti i ne zadržavaju se nakon ponovnog pokretanja poslužitelja za razmjenu poruka. Poruke koje imaju QoS razinu 1 mogu se staviti u red i zadržati nakon ponovnog pokretanja poslužitelja za razmjenu poruka. Trajnost pretplate određuje hoće li se zahtjev staviti u red čekanja. Za MQTT V5.0, trajnost se kontrolira parametrom intervala isteka sesije. Za MQTT V3.1 i V3.1.1 parametar je čista sesija. Uređaji mogu objavljivati poruke na QoS2, ali poslužitelj za upravljanje uređajima objavljuje i pretplaćuje se na QoS1, tako da su poruke odgovora samo QoS1.

Usluga platforme objavljuje zahtjeve koji imaju razinu QoS-a 1 za podršku čekanju poruka.

Za MQTT V5.0, da biste u red čekanja poslali poruke dok upravljani uređaj nije povezan, konfigurirajte uređaj da koristi trajne pretplate tako što ćete parametar čistog pokretanja postaviti na false, a parametar intervala isteka sesije na vrijednost koja nije nula. Napomena: Interval isteka sesije određuje broj sekundi za zadržavanje podataka. Mora se postaviti na odgovarajuću vrijednost koja se razlikuje ovisno o aplikaciji.

Za MQTT V3.1.1 ili V3.1, da biste na čekanje poslali poruke koje se šalju dok upravljani uređaj nije povezan, konfigurirajte uređaj da ne koristi čiste sesije postavljanjem parametra čiste sesije na false.

Upozorenje: Ako vaš upravljani uređaj koristi trajnu pretplatu, sve naredbe koje se pošalju na uređaj dok je izvan mreže prijavljuju se kao neuspjele operacije ako se uređaj ne poveže s uslugom prije isteka zahtjeva. Međutim, kada se uređaj ponovno poveže, te zahtjeve uređaj obrađuje. Za MQTT V5.0 trajna pretplata je navedena kada je parametar čistog pokretanja postavljen na false, a parametar intervala isteka sesije postavljen na nula vrijednost. Za MQTT V3.1.1 ili V3.1 trajna pretplata je navedena kada je parametar čiste sesije postavljen na false.

Teme

Upravljani uređaj mora se pretplatiti na sljedeću temu za obradu zahtjeva i odgovora usluge usluge platforme:

```
iotdm-1 / #
```

Upravljani uređaj objavljuje u temama koje su specifične za vrstu zahtjeva za upravljanje koji se izvodi:

- Upravljani uređaj objavljuje odgovore na upravljanje uređajem na iotdevice-1 / response.
- Za ostale teme na kojima upravljani uređaj može objaviti pogledajte Protokol za upravljanje uređajima i zahtjevi za upravljanje uređajima.

Format poruke.

Sve poruke šalju se u JSON formatu.

Zahtjevi (eng. requests)

Zahtjevi su oblikovani kako je prikazano u sljedećem uzorku koda:

```
{"d": {...}, "reqId": "b53eb43e-401c-453c-b8f5-94b73290c056"}
```

Gdje:

- **d** nosi sve podatke koji su relevantni za zahtjev.
- **reqId** je identifikator zahtjeva i mora se kopirati u odgovor. Ako odgovor nije potreban, možete izostaviti polje reqId.

Odgovori

Odgovori su oblikovani kako je prikazano u sljedećem uzorku koda:

```
{
    "rc": 0,
    "message": "uspjeh",
    "d": {...},
    "reqId": "b53eb43e-401c-453c-b8f5-94b73290c056"
}
```

Gdje:

- **rc** je rezultatski kod izvornog zahtjeva.
- **message** je neobavezni element s tekstualnim opisom koda odgovora.
- **d** je neobavezni element podataka koji prati odgovor.
- **reqId** je ID zahtjeva izvornog zahtjeva, koji se koristi za povezivanje odgovora sa zahtjevima. Uređaj mora osigurati da su svi ID-ovi zahtjeva jedinstveni. Odgovori na zahtjeve za uslugu platforme moraju sadržavati točnu vrijednost **reqId** zahtjeva.

3. Razvoj IoT aplikacija sa Watson IoT

Pregled Watson IoT platforme; Započinjanje sa radom u Watson IoT Platformi; Korištenje Watson IoT Platform Dashboard;

Razvoj temelja IoT aplikacije sa Node-RED I Raspberry Pi

U ovoj sekciji se možete upoznati kako da koristite IBM Cloud, Node-RED, IBM Watson IoT i Raspberry Pi za izgradnju temelja aplikacije koja koristi vremenske podatke s vremenskih senzora.

Svrha ove sekcije dad a vam pomogne u radu sa IBM Cloud ™, Node-RED, Watson® IoT i Raspberry Pi kako bi bili u mogućnosti stvoriti temelj aplikacije koja koristi vremenske podatke, poput temperature, vlažnosti i tlaka, a koje bilježi vremenski senzori.

Ovaj dio daje praktične smjernice za razvoj IoT aplikacije.

Da biste stekli razumijevanje kako izraditi IoT aplikaciju, u ovoj sekciji vi će te moći naučiti kako obaviti slijedeće zadatke:

- Definisati Raspberry Pi kao IoT uređaj u Watson IoT usluzi.
- Kako koristiti Node-RED za izradu aplikacije na Pi koja izvještava informacije o senzoru, poput temperature, vlažnosti i barometarskog tlaka, drugoj Node-RED aplikaciji koja se izvodi na IBM Cloudu.

Preduslovi

Preduslovi za obavljanje ovog zadatka su slijedeći:

- Morate imati IBM Cloud račun. Račun je besplatan i pruža pristup svemu što vam je potrebno za razvoj, praćenje, planiranje i postavljanje aplikacija. Prijavite se za suđenje. Za račun je potreban IBMid. Ako nemate IBMid, možete ga stvoriti kad se registrirate.
- Vaš IBM Cloud račun mora imati najmanje 8 GB vremena izvođenja i memorije spremnika, plus pristup pružanju do 10 usluga.
- Morate imati instancu usluge Internet of Things Platform.
- Morate imati primjerak usluge Db2 Warehouse on Cloud.
- Morate imati Raspberry Pi i SENS HAT.
- Morate se moći povezati s mrežom Raspberry Pi i trebate znati IP adresu.

- Morate ažurirati Node.js i Node-Red na Raspberry Pi pokretanjem naredbe update-nodejs-and-nodered u terminalu na Raspberry Pi.
- Morate imati program SSH terminala da biste se povezali s Raspberry Pi. Ako koristite MacOS ili Linux sustav, SSH terminal program je već instaliran. Ako koristite sustav Windows, instalirajte aplikaciju PuTTY koja je dostupna na http://www.putty.org.

Zadatak 1: Stvaranje usluge platforme Internet of Things

1. Otvorite preglednik i prijavite se na jedan od računa IBM Cloud računa vašeg tima na https://cloud.ibm.com.

   Otvara se nadzorna ploča vaših aplikacija.

2. Pritisnite dugme **Create resource**.
3. Kliknite uslugu **Internet of Things Platform**.

   Savjet: Da biste brzo pronašli uslugu, upotrijebite značajku za upisivanje u traku za pretraživanje. Obavezno kliknite uslugu IoT Platform, a ne IoT platformu.

4. Upišite naziv za svoj primjerak usluge IoT Platform. Predlaže se zadani naziv, ali možete ga zamijeniti. Iako usluzi možete imenovati bilo što, u primjerima ovog tečaja naziv usluge je myWorkshop-IoT.
5. Kliknite **Create**. Nakon trenutka prikazuje se stranica Pojedinosti o usluzi vaše nove usluge IoT Platform.

Zadatak 2: Definirajte Raspberry Pi uređaj na usluzi IoT Platform

U ovaj zadatak dodajete uređaje potrebne IoT aplikaciji.

1. Ako još niste otvorili svoju IoT platformu, otvorite je:

   a. Prijavite se na jedan od IBM Cloud računa vašeg tima na https://cloud.ibm.com. Prikazana je nadzorna ploča vaših aplikacija.

   b. Pomaknite se do odjeljka Sve usluge i kliknite svoju uslugu IoT Platform. Prikazuje se stranica sa detaljima usluge vaše usluge IoT Platform.

2. Kliknite **Launch**.

   Usluga IoT Platform otvara se na zasebnoj kartici preglednika, ostavljajući stranicu Pojedinosti IoT usluge otvorenom. Držite stranicu Pojedinosti usluge otvorenom kako biste se kasnije mogli lako vratiti na nadzornu ploču IBM Cloud.

3. Stvorite IoT Gateway uređaj u usluzi IoT Platform koji će predstavljati Raspberry Pi. U lijevoj navigacijskoj ploči kliknite ikonu uređaja koja izgleda ovako:

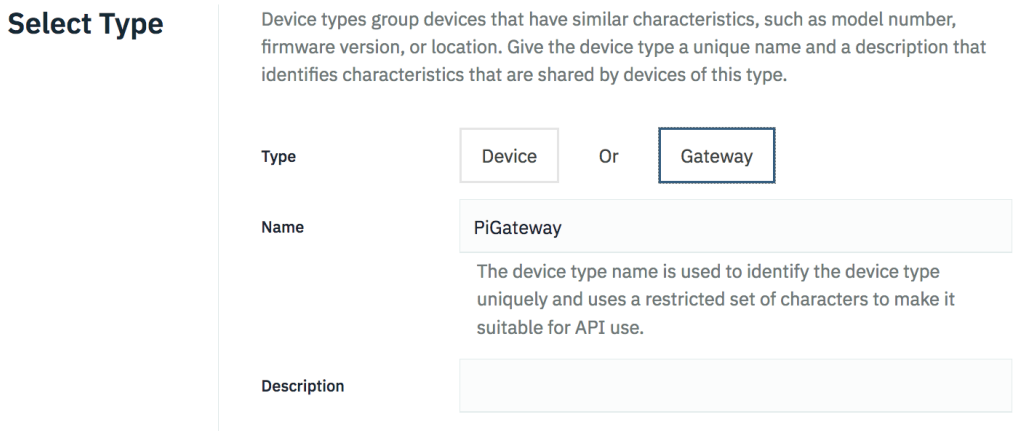
Otvara se stranica Uređaji.

Napomena: Ovaj projekat Raspberry Pi tretira kao pristupnik, a priloženi Sense HAT kao downstream senzor. Međutim, kao što ćete vidjeti, Sense HAT ne trebate definirati za uslugu IoT Platform, jer ga gateway uređaj definira za vas kad se Sense HAT poveže preko njega.

4. Kliknite Add Device

5. .Prvi korak stvaranja uređaja je odabir vrste uređaja. Nije dostupna nijedna vrsta uređaja, pa je morate stvoriti. Kliknite karticu **Device Types**, a zatim pritisnite dugme **Add Device**.

6. Budući da ćete Raspberry Pi konfigurirati kao gateway uređaj, kliknite **Gateway** i upišite `PiGateway` za njegovo ime.



7. Kliknite **Next**.

Prikazuje se stranica Definiraj predložak. Na ovoj stranici možete odabrati atribute za vrstu uređaja. Svi su atributi neobavezni. Koriste se kao predložak za sve nove uređaje koji koriste ovu vrstu uređaja. Ako uređaj koristi ovu vrstu uređaja,

njegove se atribute mogu uređivati pojedinačno, čak i ako ih ne definirate u predlošku.

8. Ne trebate definirati nikakve atribute, pa kliknite Next.

   Prikazuje se stranica `Submit Information page`. Da ste na prethodnoj stranici odabrali bilo koji atribut, oni bi ovdje bili navedeni za provjeru.

9. Kliknite **Next** da biste otvorili stranicu Metapodaci.

   Na stranici Metapodaci možete definirati bilo kakve prilagođene atribute koji bi mogli biti potrebni za vaše okruženje.

10. Ne trebaju vam metapodaci, pa kliknite **Create** za stvaranje nove vrste uređaja `PiGateway`.

    Prikazuje se stranica `Add Device`, a nova vrsta uređaja, PiGateway, nalazi se na popisu vrsta uređaja.

11. Odaberite vrstu uređaja PiGateway i kliknite **Next**.

    Prikazuje se stranica s podacima o uređaju. Svaki uređaj treba jedinstveni ID unutar instance usluge IoT Platform; ID-ovi su definirani na ovoj stranici. Možete koristiti bilo koje jedinstveno ime. U primjerima ovog tečaja, ID uređaja je `myPiGateway`.

    Napomena: Na ovoj stranici možete definirati nekoliko drugih atributa kako biste identificirali uređaj i njegovu svrhu. Ti atributi mogu biti korisni u okruženju s više uređaja. Međutim, budući da u ovom tečaju koristite samo jedan pristupnik i jedan nizvodni uređaj, ti drugi atributi ne trebaju.

12. Upišite ID uređaja i kliknite **Next**.

    Prikazuje se stranica Metapodaci. Na ovoj stranici možete definirati bilo kakve prilagođene atribute koji bi mogli biti potrebni za vaše okruženje.

13. Ne trebaju vam nikakvi metapodaci, pa kliknite **Next** da biste otišli na stranicu Sigurnost.

    Što se tiče sigurnosti, imate dvije mogućnosti. Automatski generirani token slučajni je, kombinacija alfanumeričkih znakova i simbola od 8 do 36 znakova. Samopomoćni token daje vam mogućnost da za uređaj osigurate vlastiti token za provjeru autentičnosti.

14. Iako je u stvarnosti sigurnost najvažnija, za ovaj tečaj pomaknite se prema dolje i upišite lako pamtljivi, samopomoćni žeton, poput maline. Kliknite **Next**.

Važno: Tokeni provjere autentičnosti šifrirani su i ne mogu se oporaviti ako su izgubljeni. Obavezno zabilježite svoj token.

15. Na stranici `Summary page` provjerite sve svoje unose. Izvršite izradu uređaja klikom na **Add**.

16. Vaš je uređaj sada definiran i prikazuje se stranica sa sažetkom. Na stranici sažetka zabilježite sljedeće stavke; trebat će vam kad svoj uređaj povežete s uslugom IoT Platform.

    ID organizacije: _____

    Tip uređaja: _____

    ID uređaja: _____

    Token: _____

17. Zatvorite `summary`.

Prikazuje se nadzorna ploča uređaja, na kojoj možete vidjeti svoj novi uređaj. Ostavite ovu karticu preglednika otvorenom za kasnije provjeru valjanosti. Prebacite se na stranicu Pojedinosti IoT usluge kako biste se mogli vratiti na svoju nadzornu ploču IBM Cloud.

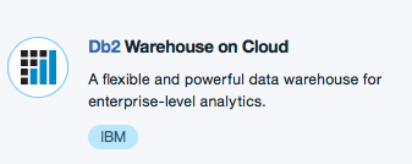
Da biste se vratili na nadzornu ploču IBM Cloud, kliknite IBM Cloud.

Zadatak 3: Stvorite Db2 skladište na usluzi Cloud

Ako ste dovršili preduvjet za stvaranje usluge Db2 Warehouse on Cloud, možete preskočiti na 4. zadatak i nastaviti s definiranjem tablice Db2 Warehouse. U suprotnom, slijedite ove korake za stvaranje usluge Db2 Warehouse on Cloud:

1. Na vašoj nadzornoj ploči IBM Cloud kliknite dugme **Create resource**.

2. Kliknite uslugu Db2 Warehouse on Cloud.



Savjet: Da biste brzo pronašli uslugu, upotrijebite značajku za upisivanje teksta na traku za pretraživanje.

3. Upišite naziv za svoju instancu usluge DbB Warehouse on Cloud. Predlaže se zadani naziv, ali možete ga zamijeniti. Iako uslugu možete imenovati bilo kako, primjeri u ovom primjeru koristimo `myWorkshop-Db2` kao naziv usluge Db2 Warehouse on Cloud.

4. Kliknite **Create**.

5. Nakon trenutka prikazuje se vaša nadzorna ploča IBM Cloud. Vaša usluga Db2 Warehouse on Cloud je spremna.

Zadatak 4: Kreirajte Db2 Warehouse tabelu za podatke o okolišu

Morate stvoriti tablicu u usluzi Db2 Warehouse on Cloud kako biste čuvali podatke o okolišu koji se vašoj aplikaciji šalju iz senzora Sense HAT. Tablica će pohraniti vrijednosti temperature, vlage i barometarskog tlaka u red svaki put kad se primi neki okolišni događaj. Također će pohraniti ID senzora koji je poslao podatke i vremensku oznaku.

1. Pronađite uslugu `myWorkshop-Db2` na svojoj nadzornoj ploči IBM Cloud i kliknite je da biste je otvorili.

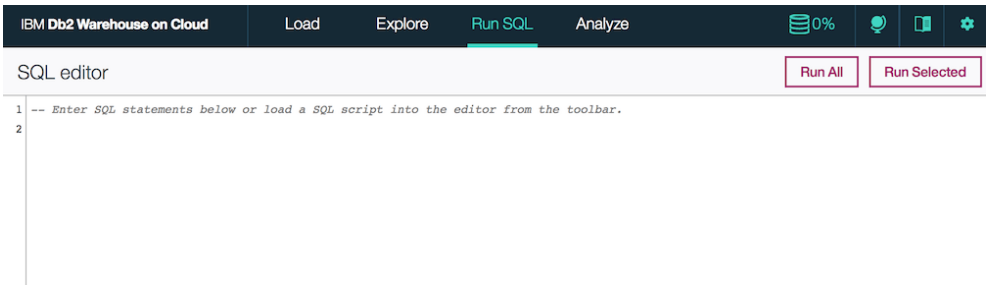
   Prikazuje se stranica Pojedinosti o usluzi vaše usluge Db2 Warehouse on Cloud.

2. Pritisnite **OPEN**.

   Usluga Db2 Warehouse on Cloud otvara se u zasebnom prozoru ili kartici preglednika, ostavljajući stranicu Pojedinosti usluge otvorenom.

   Savjet: Držite stranicu Pojedinosti usluge otvorenom tako da se lako možete vratiti na svoju nadzornu ploču IBM Cloud.

3. Kliknite tab **Run SQL**



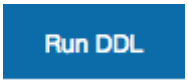
4. Unesite ovaj tekst:

```
CREATE TABLE "SENSEDATA"
(
"SENSORID" VARCHAR(20),
```

```
"TEMPERATURE" DOUBLE,
"HUMIDITY" DOUBLE,
"PRESSURE" DOUBLE,
"TIMESENT" TIMESTAMP
);
```

Napomena: Naziv ove tablice i nazivi redaka bit će važni elementi kasnije, zato svakako provjerite pravopis.

5. Kliknite **Run All**.



6. S popisa naziva tablice odaberite **SENSEDATA**.

Prikazuje se definicija tablice. Da biste pregledali podatke, možete otići na **Explore**, odabrati shemu i tablicu, a zatim kliknuti **View Data**.

7. Ostavite ovu karticu preglednika otvorenom za kasnije provjeru valjanosti. Prebacite se na stranicu Db2 Warehouse na Cloud Service Details kako biste se mogli vratiti na vašu nadzornu ploču IBM Cloud.

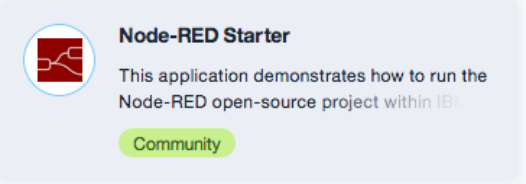
8. Da biste se vratili na nadzornu ploču IBM Cloud, kliknite **IBM Cloud**.

Zadatak 5: Stvaranje prostora aplikacije IBM Cloud Node-RED

Vrijeme je da stvorimo IBM Cloud stranu aplikacije: Node-RED aplikaciju koja prima događaje senzora od i šalje naredbe na Raspberry Pi. Počet ćete s predloškom (eng. boilerplate) prijave za Node-RED i povezati IoT platformu i Db2 Warehouse na Cloud uslugama. Zatim ćete otvoriti terminal za svoj Raspberry Pi.

1. Na vašoj nadzornoj ploči IBM Cloud pomaknite se do odjeljka Sve aplikacije. Kliknite **Create App**.

2. Pritisnite tipku Node-RED Starter boilerplate



Savjet: Da biste brzo pronašli pločicu, upotrijebite značajku za navođenje vrste trake za pretraživanje.

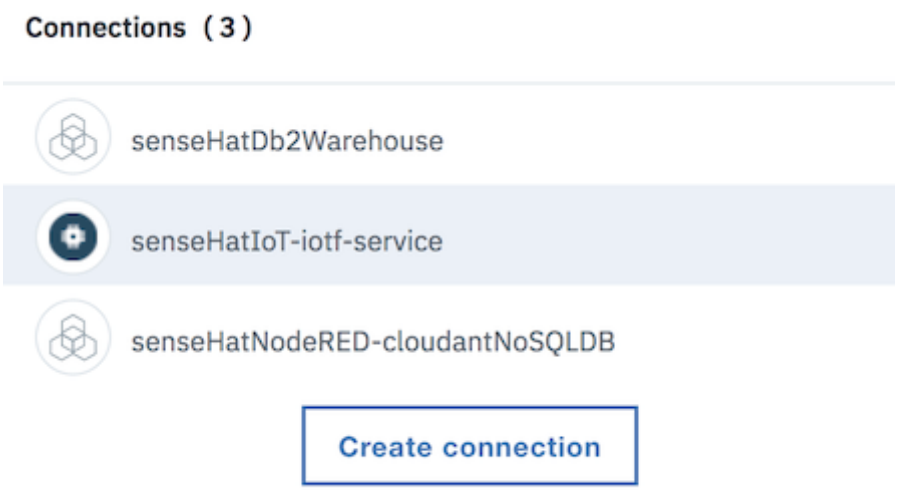
3. Na rezultirajućoj stranici upišite ime nove aplikacije. Možete imenovati bilo koju aplikaciju ako je ime jedinstveno u prostoru. Primjeri u ovom vodiču koriste `myWorkshop-xxx`.

   Nakon što upišete naziv aplikacije, ostala polja ostavite onakva kakva jesu i kliknite **Create**.

   Aplikacija je kreirana. Nakon nekoliko trenutaka prikazuje se stranica **Getting Started**.

4. Stvorite veze s vašom IoT platformom i Db2 Warehouseom on Cloud. Idite na odjeljak Veze na stranici aplikacije. Kao dio Node-RED Starter uzorka, automatski je stvorena usluga baze podataka Cloudant NoSQL. Baza podataka Cloudant NoSQL sadrži sav vaš aplikacijski kôd. U ovom su odjeljku dodane veze s vaše dvije usluge.

5. Kliknite **Create connection**.



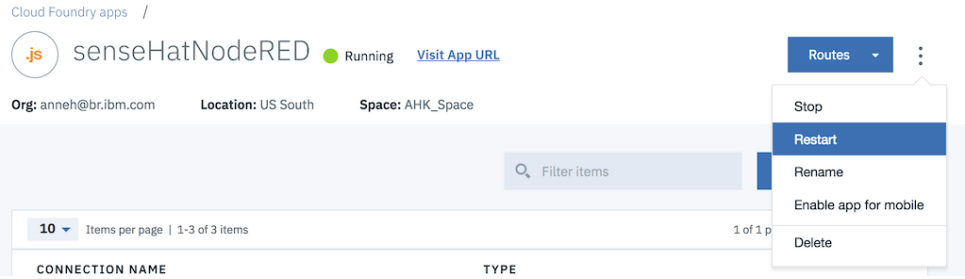
6. S popisa usluga odaberite svoju uslugu IoT Platform, myWorkshop-IoT.

   Kliknite **Connect**.

7. Kad se prikaže zahtjev za ponovnim prijavljivanjem, kliknite **Cancel**.

8. Ponovite korake 5 i 6 za uslugu Db2 Warehouse on Cloud, `myWorkshop-Db2`.

9. Kad se prikaže zahtjev za ponovnim stavljanjem, kliknite meni i **Restart.**



Prikazuje se odjeljak Veze vaše aplikacije.

10. Kliknite **Overview** da biste vidjeli stranicu Overview page.

Ostavite ovu karticu preglednika otvorenom kako biste se mogli lako vratiti na nju.

Zadatak 6: Stvaranje protoka Raspberry Pi Čvor-CRVENI

U ovom zadatku izrađujete Node-RED aplikaciju na Raspberry Pi. Ta će aplikacija prikupljati podatke senzora sa Sense HAT uređaja koji je priključen na Pi. Zatim te podatke prosljeđujete na svoju IoT Platform uslugu kako bi ih podatke mogla koristiti odgovarajuća Node-RED aplikacija koju ćete stvoriti na IBM Cloudu.

Tri vrste podataka senzora - okruženje, kretanje i joystick - šalju se usluzi IoT Platform s određenom vrstom događaja tako da se mogu poduzimati različite radnje ovisno o vrsti događaja.

Node-RED aplikacija može primati naredbe od IBM Cloud aplikacije koja kontrolira 8x8 LED matricu koja je dio Sense HAT uređaja. Naredba alarma može pretvoriti cijelu matricu u jednobojnu boju koja se pruža kao dio korisnog tereta poruke. Naredba poruke može pomicati tekstualnu poruku preko matrice. Poruka, boja teksta i boja pozadine pružaju se kao dio korisnog tereta poruke.

Prije nego što možete stvoriti aplikaciju Node-RED na Raspberry Pi, provjerite je li Raspberry Pi uključen i je li pokrenuta usluga Node-RED.

1. Napajajte svoj Raspberry Pi pričvršćivanjem standardnog microUSB kabela između microUSB konektora na Raspberry Pi i izvora napajanja poput prijenosnog računala ili USB bloka napajanja. Uključivanje uređaja traje manje od minute.

2. Provjerite je li SSH instaliran i konfiguriran pokretanjem naredbe **`sudo systemctl start ssh`**. Ako naredba vrati poruku o pogrešci, slijedite ove korake za instaliranje i konfiguriranje SSH-a.

   a. U prozor terminala upišite sudo raspi-config.

   b. Odaberite **Interfacing Options**.

   c. Odaberite **SSH**.

   d. Kliknite **Yes**, a zatim **OK**.

   e. Pritisnite **Finish**.

3. Povežite se s Raspberry Pi pomoću SSH-a. Do vašeg Pi-a može se doći putem njegove IP adrese pomoću ovog formata: **`ssh pi @ <ip adresss>`**.

   Da biste pronašli IP adresu, **`hostname –I`**

   Napomena: Ovisno o konfiguraciji sustava, možda ćete se moći povezati s prijenosnim računalom imenom, a ne ip adresom. Da biste to učinili, dodajte naziv **`.local`** svom nazivu hosta Raspberry Pi. Na primjer: **`ssh pi@raspberrypi.local`** (**`pi`** je zadano korisničko ime na Raspberry Pi).

   - Ako koristite MacOS ili Linux sustav, otvorite prozor naredbenog retka da biste pokrenuli ssh naredbu.
   - Ako koristite sustav Windows®, pokrenite aplikaciju PuTTY s izbornika Start sustava Windows i navedite podatke o povezivanju.

4. Kada se od vas zatraži korisnička lozinka, unesite vjerodajnice za Raspberry Pi:

   - User ID: pi
   - Password: raspberry (po vašem izboru)

   Napomena: Kada se prvi put povežete s Raspberry Pi, možda ćete vidjeti poruku koja ukazuje na to da nije moguće utvrditi autentičnost hosta. Odgovorite "da".

5. Kad se od vas zatraži da promijenite lozinku svog Pi, upotrijebite naredbu passwd da biste je promijenili kako biste osigurali sigurnost svog rada. Obavezno zabilježite novu lozinku.

6. Instalirajte **node-red-node-pi-sense-hat**.

   a. Otvorite NodeRed.

   b. U odjeljak **Palette/Install** upišite **`sense-hat`** u okvir za pretraživanje,

   c. Kliknite **Install** i pričekajte da se promjena statusa instalira.

7. Da biste osigurali da će se Node-RED automatski ponovo pokrenuti u slučaju ponovnog pokretanja ili rušenja, omogućite uslugu Node-RED unosom ove naredbe:

   ```
   sudo systemctl omogućiti nodered.service
   ```

8. Pokrenite Node-RED na Pi unošenjem ove naredbe:

   ```
   node-red-start
   ```

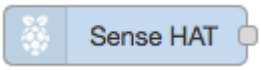
   Savjet: Kada se pokrene Node-RED aplikacija, zadnja radnja je pokretanje funkcije bilježenja. Ako želite, iz ove evidencije možete izaći pritiskom na Ctrl + C. Sam Node-RED se neće zaustaviti. Ako ili kada želite zaustaviti Node-RED, unesite **node-red-stop**.

Važno je da raumijete način na kokoji se programiraju dva toka podataka na node-RED.

Tok 1: slanje podataka senzora

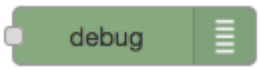
1. Programiranje NOD-RED vrši se na web pregledniku. Da biste započeli, na drugom prijenosnom računalu otvorite web preglednik i unesite ip-adresu: **1880**, gdje je ip adresa IP adresa vašeg Raspberry Pi.

2. Iz palete čvorova s lijeve strane pronađite ulazni čvor Sense HAT koji se nalazi u odjeljku **Raspberry_Pi palete** i povucite ga u svoj radni prostor Node-RED.

3. Dvaput kliknite novi Sense HAT node da biste otvorili njegove postavke. Potvrdite svaki okvir da biste prijavili sve tri vrste događaja.

4. U izlaznom odjeljku pronađite čvor za uklanjanje pogrešaka. Dodajte ga s desne strane Sense HAT node.

5. Otvorite postavke za uklanjanje pogrešaka i promijenite izlaz da biste dovršili objekt poruke (**`complete msg object`**), tako da možete pregledati cijelu poruku koju je primio prethodni čvor. To može biti korisno za formatiranje poruke koja se šalje na sljedeći node.

6. Povežite svoj Sense HAT node s vašim čvorom za otklanjanje pogrešaka (debug node) povlačenjem s jedne točke povezivanja na drugu.

7. Potvrdite da vaš Sense HAT daje izlaz klikom na dugme **Deploy**.

8. Na desnoj strani stranice pronađite karticu za uklanjanje pogrešaka (**Debug**). Kliknite tu karticu. Velika količina podataka počinje dolaziti do vašeg čvora za otklanjanje pogrešaka iz Sense HAT-a.

9. Na desnoj strani noda za uklanjanje pogrešaka pronađite zeleni prekidač.

Prekidač možete koristiti za zaustavljanje ili pokretanje izlaza na taj određeni čvor za uklanjanje pogrešaka. Isključite izlaz klikom na prekidač. Podaci se prestaju pomicati na ploči za uklanjanje pogrešaka. Ispitajte stvarne poruke koje SENS HAT šalje. Svaka poruka Sense HAT-a ima temu i korisni teret. Tema se podudara s jednom od tri vrste podataka koje Sense HAT izvještava: okoliš, pokret i džojstik. Da biste izvršili radnje na temama senzora, morate ih razdvojiti u jedinstvene događaje.

10. U odjeljku funkcija pronađite preklopni node i dodajte ga u svoj radni prostor desno od vašeg čvora Sense HAT.

11. Spojite preklopni čvor na čvor Sense HAT. Preklopni čvor ima konektore i na lijevoj i na desnoj strani. Preklopni čvor uzima dolaznu poruku s lijeve strane i usmjerava tijek aplikacije na različite staze na temelju vrijednosti elementa dolazne poruke. Čvor tada šalje poruku pomoću izlaznih konektora s desne strane.

12. Otvorite postavke za preklopni čvor i postavite vrijednost svojstva na **`msg.topic`**. Sadržaj msg.topic koristi se za grananje tijeka aplikacije. Nakon što je vrijednost **`property`** područje u kojem možete odrediti s čime želite usporediti **`msg.topic`**. Ova aplikacija treba usmjeravati svoj tok na temelju toga je li msg.topic jednak (==) **`environment`**, **`motion`** ili **`joystick`**.

13. Kliknite meni pored znaka jednakosti (==) da biste dobili ideju o mogućim operacijama usporedbe koje se mogu obaviti. Ostavite vrijednost postavljenu na ==. Desno od znaka jednakosti (==) nalazi se polje u kojem odredite vrijednost s kojom ćete uspoređivati. Možete odabrati s popisa da odredite koju vrstu podataka se uspoređuje.

14. Obavezno odaberite **`String`** i unesite niz **`environment`** string u polje.

15. Pritisnite **add** da biste dodali polja za usporedbu **motion** i **joystick**.

Napomena: Kada zatvorite postavke sklopnog čvora, na izlaznoj strani preklopnog čvora prikazuju se tri odvojene točke spajanja. Te točke upotrebljavate za usmjeravanje toka na temelju rezultata usporedbe. Točke spajanja su istim redoslijedom kao u postavkama sklopnog čvora.

16. Dodajte dva **delay node**. Kada ste pregledavali izlaz za otklanjanje pogrešaka, vjerojatno ste primijetili količinu događaja koje generiraju i okolina i teme pokreta. Ako ste svaki od tih događaja poslali na uslugu IoT Platform, brzo biste potrošili ograničenje podataka od 200 MB vaše besplatne usluge IoT Platform. Da biste se nosili s tim, možete dodati dva čvora odgode. Spojite jedan na izlaz okoline, a jedan na izlaz kretanja sklopnog čvora.

17. Za svaki čvor odgode otvorite postavke i postavite radnju na **Limit rate to**.

18. Ograničite brzinu na 1 poruku svakih 5 sekundi i označite potvrdni okvir **drop intermediate messages**. Program će odbaciti sve poruke, osim jedne svakih 5 sekundi.

19. Premjestite čvor za otklanjanje pogrešaka iz Sense HAT-a na izlaz čvorova prekidača / kašnjenja:

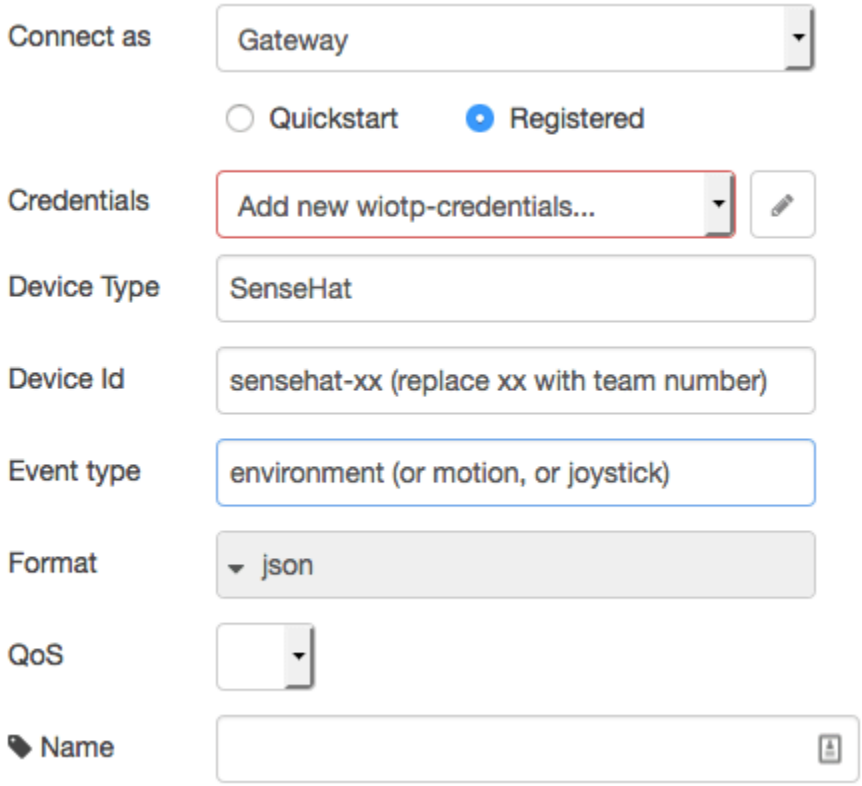
    - Izbrišite vezu između čvora Sense HAT i čvora za uklanjanje pogrešaka klikom na liniju koja ih povezuje i pritiskom na Delete.
    - Spojite izlaz dva čvora odgode i konačnu vezu prekidača, tema joysticka, na čvor za uklanjanje pogrešaka.

    Savjet: Nekoliko čvorova može se povezati s jednom točkom povezivanja na drugom čvoru.

20. Ponovno rasporedite aplikaciju klikom na **Deploy**. Broj primljenih poruka počinje se smanjivati.

    Napomena: Kada koristite joystick Sense HAT, vidjet ćete samo teme o joysticku. Iz tog razloga ne trebate odgađati te poruke kao za ostale teme.

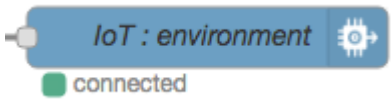
21. Pošaljite ove poruke svojoj IoT Platform usluzi kako bi im se moglo pristupiti iz vašeg IBM Cloud programa. Da biste to učinili, morate povući tri izlazna čvora Watson IoT u svoj radni prostor i postaviti ih desno od čvorova kašnjenja. Svaki IoT čvor šalje zasebnu vrstu događaja usluzi IoT Platform. Konfigurirajte čvorove otvaranjem njihovih postavki i konfiguriranjem na sljedeći način:



- Budući da ste Raspberry Pi definirali kao gateway uređaj, na popisu **Connect as** (Poveži kao) odaberite **Gateway** (Pristupnik).
- Kada konfigurirate prvi od ovih čvorova, odaberite Dodaj nove **wiotp-credentials** i kliknite ikonu olovke.
- Navedite gateway uređaj koji ste prethodno definirali. U odgovarajuća polja unesite vrijednosti koje ste zabilježili tijekom definicije IoT uređaja. Nemojte mijenjati nijedno drugo polje.
- Vrsta uređaja i ID mogu biti bilo koje vrijednosti koje pomažu prepoznati njihovu svrhu. Koristite navedene vrijednosti.
- Vrijednost u polju **Event type** definira događaj koji ova poruka sadrži. Upotrijebite jednu od tri vrijednosti u svakom čvoru.

22. Povežite tri IoT čvora s odgovarajućim čvorovima za odgodu ili prebacivanje.

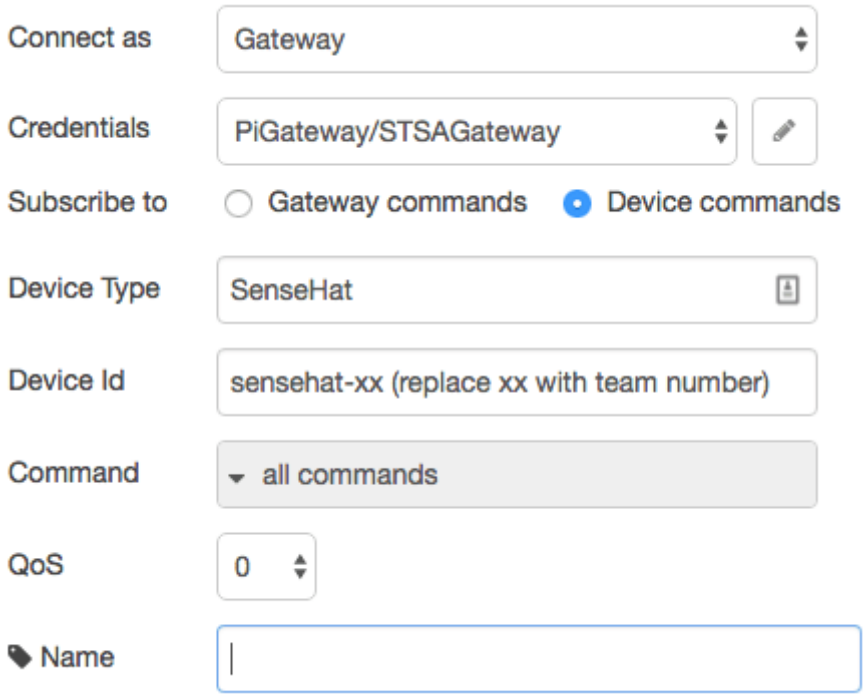
23. Pokrenite aplikaciju. Zelena točka u blizini IoT čvorova znači da su povezani s uslugom IoT Platform.



Tok 2: Primite IoT naredbe

Drugi tok prima naredbe koje kontroliraju Sense HAT LED. Da biste izgradili protok, potrebna su vam četiri čvora: Watson IoT ulazni čvor povezuje se s funkcijskim čvorom, koji se povezuje s izlaznim čvorom Sense HAT i čvorom za otklanjanje pogrešaka.

1. U prostor nakon prvog toka povucite ove čvorove u svoj radni prostor i povežite ih. Savjet: Ne morate stvoriti ovaj drugi tok na zasebnoj kartici. Možete koristiti prostor nakon prvog toka.
2. Postavite čvor za otklanjanje pogrešaka tako da prikazuje cijeli objekt poruke.
3. Konfigurirajte IoT ulazni čvor za primanje naredbi koje se šalju iz aplikacije IBM Cloud. Otvorite postavke i konfigurirajte čvor na sljedeći način:



- Budući da ste Raspberry Pi definirali kao gateway uređaj, na popisu **Connect as** (Poveži kao) odaberite **Gateway** (Pristupnik).
- Za postavku **Subscribe to** kliknite **Device command** jer ovaj čvor osluškuje naredbe koje su namijenjene daljnjem uređaju, a ne sam pristupnik.
- c. S liste **Command** odaberite **all commands**. Za razliku od drugog toka, sve ćete naredbe uhvatiti jednim IoT čvorom. U ovom slučaju i dalje poduzimate različite radnje na temelju vrste naredbe, ali vrstu naredbe određujete JavaScript kodom u sljedećem čvoru. Također možete odrediti vrstu naredbe pomoću dva zasebna IoT čvora, po jedan za svaku naredbu,

kao što ste to učinili za izlazne događaje. Možete izvršiti isti zadatak na mnogo različitih načina pomoću Node-RED.

- Funkcija node moćan je čvor koji možete koristiti za ugradnju svoje programske logike u Node-RED aplikaciju. Poruka se prenosi čvoru funkcije kao JavaScript objekt koji se naziva **msg**. Po dogovoru ima svojstvo **msg.payload** koje sadrži tijelo poruke. Možete djelovati na sadržaj ovog korisnog tereta, izmijeniti ga i proslijediti sljedećem čvoru u svojoj aplikaciji. Čvor funkcije u ovom tijeku prima poruku od IoT čvora i stavlja je u format koji Sense HAT očekuje. Objekti **msg** koji dolaze iz IoT čvora su u ovom formatu:

```
The "alarm" command:


msg.command: "alarm"
msg.format: "json"
msg.deviceType: "SenseHat"
msg.deviceId: "sensehat-xx"
msg.payload: {d:{color:msg.payload}}
The "message" command:


msg.command: "message"
msg.format: "json"
msg.deviceType: "SenseHat"
msg.deviceId: "sensehat-xx"
msg.payload: {d:{color:"blue",
background:"green",
message:"message text"}}
```

Da bi cijelu 8x8 Sense HAT LED matricu postavili na određenu boju, čvor Sense HAT očekuje ovaj niz kao **msg.payload**:

```
msg.payload = "\*, \*, *color*"
(replacing *color* with a color choice like red,
blue, green, etc)
```

Za pomicanje poruke kroz LED matricu, format msg.payload je detaljniji:

```
msg.color = "*color*"
(replacing *color* with a color choice like red,
blue, green, etc)


msg.background = "*color*"
(replacing *color* with a color choice like red,
blue, green, etc)


msg.payload = "message to display"
```

```
//(If the message string is only a single
character, it will not scroll
```

Znanjem sadržaja dolaznog formata msg i zahtjevima Sense HAT-a, isječak JavaScript koda može provjeriti vrstu naredbe i izvršiti transformaciju.

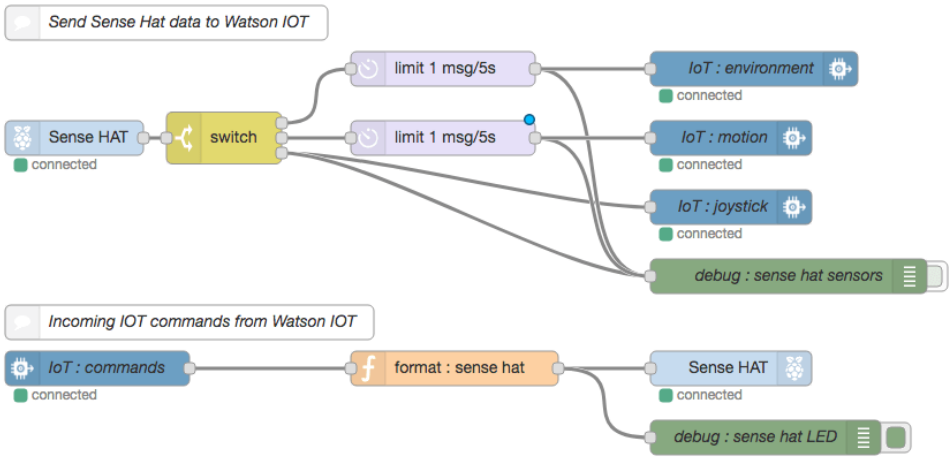
4. Unesite ovaj kod u funkcijsko polje funkcijskog čvora:

```
// begin code
d = msg.payload.d;
if (msg.command == "message") {
msg.background = d.background;
msg.color = d.color;
msg.payload = d.message;
}
else if (msg.command == "alarm") {
msg.payload = "\*,\*," + d.color;
}
else
msg = null;
return msg;
// end code
```

Raspberry Pi strana ove aplikacije je potpuna.

5. Kliknite Deploy da biste pokrenuli aplikaciju. Nakon završetka IBM Cloud stranice, možete testirati protoke i osigurati da sve funkcionira prema očekivanjima. Zadatak 8 uključuje nekoliko testova za provjeru koje možete koristiti.

6. Provjerite izgleda li vaša aplikacija Raspberry Pi na sljedećem primjeru:



Zadatak 7: Stvaranje IBM Cloud Node-RED tokova

U ovom zadatku kreirate Node-RED aplikaciju na IBM Cloudu koja će primati podatke senzora iz odgovarajuće aplikacije na Raspberry Pi. Zatim neke od tih podataka pohranite u uslugu Db2 Warehouse on Cloud kako bi se podaci mogli koristiti u kasnijim zadacima.

Primljene su tri vrste podataka senzora - okoliš, pokret i džojstik. U bazu podataka pohranjujete samo podatke o okolini. Događaji pokreta i džojstika završavaju u čvoru za otklanjanje pogrešaka tako da možete provjeriti jesu li primljeni.

Ovaj program šalje naredbe aplikaciji Raspberry Pi koja kontrolira 8x8 LED matricu koja je dio Sense HAT uređaja. Naredba alarma pretvara cijelu matricu u jednobojnu boju koja se pruža kao dio korisnog tereta poruke. Naredba za poruku pomiče tekstualnu poruku preko matrice. Poruka, boja teksta i boja pozadine pružaju se kao dio korisnog tereta poruke.

Tok 1: Primanje IoT događaja

1. Programiranje NOD-RED vrši se na web pregledniku. Da biste započeli, vratite se na stranicu Pregled vaše IBM Cloud aplikacije, koju ste ostavili otvorenu na kraju 5. zadatka.

2. Idite na programski prostor Node-RED programa klikom na Visit App URL.

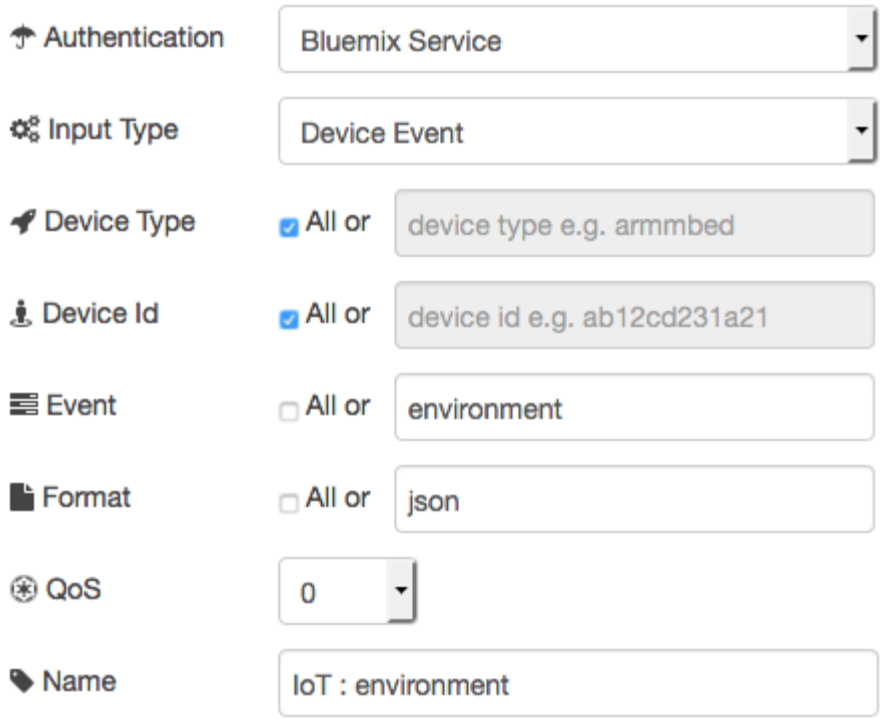
3. Kada prvi put pokrenete Node-RED okruženje, prikazuje se čarobnjak za dobrodošlicu. Kliknite **Next** da biste prošli kroz čarobnjak. Važno: Kada se od vas zatraži da postavite korisničko ime i lozinku kako biste osigurali svoj Node-RED prostor, ne morate postaviti te vjerodajnice. Međutim, ako ih ne postavite, mogli biste izgubiti sav rad na ovoj aplikaciji i morati početi ispočetka.

4. Nakon što dovršite čarobnjaka, prikazuje se stranica za pokretanje Node-RED. Pokrenite uređivač klikom na **Go to your Node-RED flow editor**.

5. Iz odjeljka za unos palete čvorova pronađite ulazni čvor ibmiot i povucite ga u svoj radni prostor Node-RED.

   Ulazni čvor ibmiot prima događaje koji se šalju iz aplikacije Raspberry Pi.

6. Dvaput kliknite čvor ibmiot da biste otvorili i konfigurirali njegove postavke.



- Obavezno odaberite IBM Cloud Service za postavku Autentifikacije. Budući da je usluga IoT Platform povezana s vašom aplikacijom, svim se provjerama autentičnosti može rukovati putem IBM Cloud-a. Za autentifikaciju ne trebaju biti dostavljeni drugi podaci.
- Postavite ovaj čvor da prihvaća događaje svih vrsta uređaja i ID-ove uređaja. Ako je potrebno, možete biti restriktivni i prihvatiti samo događaje s određenim ID-ovima i vrstama.
- Postavite ovaj čvor da prihvaća samo događaje tipa okoline. Stvorit ćete druge čvorove za upravljanje džojstikom i događajima pokreta.

7. Nakon ibmiot čvora dodajte još dva ibmiot čvora: jedan za obradu događaja kretanja i jedan za događaj upravljačke palice.
8. U izlaznom odjeljku pronađite čvor za uklanjanje pogrešaka. Dodajte ga desno od ibmiotovih čvorova.
9. Otvorite postavke otklanjanja pogrešaka i promijenite izlaz **`complete msg object`** tako da možete pregledati cijelu poruku koju je primio prethodni čvor. To može biti korisno za formatiranje poruke koja se šalje na sljedeći čvor.
10. Povežite svoje ibmiot čvorove s vašim čvorom za otklanjanje pogrešaka povlačenjem s jedne točke povezivanja na drugu. Savjet: Nekoliko čvorova može se povezati s jednom točkom povezivanja.

11. Da biste osigurali da je strana ovog projekta s Raspberry Pi dovršena, provjerite primate li događaje s Raspberry Pi klikom na **Deploy**.

12. Kliknite karticu **debug**. Podaci teku u vaš čvor za otklanjanje pogrešaka s ibmiot čvorova.

13. Na desnoj strani čvora za uklanjanje pogrešaka pronađite zeleni prekidač.

Prekidač možete koristiti za zaustavljanje i pokretanje izlaza na taj čvor za ispravljanje pogrešaka. Isključite izlaz klikom na prekidač. Podaci prestaju dolaziti na ploču za uklanjanje pogrešaka. Ispitajte primljene poruke događaja. Svaka poruka ima korisni teret i vrstu događaja koja se podudara s jednim od tri događaja koja Raspberry Pi prosljeđuje: okoliš, pokret i džojstik. Savjet: Sadržaj kartice za uklanjanje pogrešaka možete isprati klikom na ikonu koša za smeće u gornjem desnom kutu.

14. Spremite podatke o dolaznom okruženju u tablicu Db2 Warehouse. Prvo, morate smjestiti dolazne podatke u ispravan format baze podataka pomoću čvora funkcije. Iz odjeljka Funkcija dodajte čvor funkcije u svoj radni prostor i spojite ga s desne strane čvora IoT okoline. Napomena: Funkcijski čvor ima konektore i na lijevoj i na desnoj strani. Ovaj čvor prima dolaznu poruku s lijeve strane, modificira je i šalje poruku s izlaznog konektora na desnoj strani.

15. Upotrijebite funkcijski čvor za postavljanje poruke u format koji očekuje usluga Db2 Warehouse. Čvor funkcije snažan je čvor koji možete koristiti za ugradnju svoje programske logike u Node-RED aplikaciju. Poruka se prenosi čvoru funkcije kao JavaScript objekt koji se naziva **`msg`**. Po dogovoru ima svojstvo **`msg.payload`** koje sadrži tijelo poruke. Možete djelovati na sadržaj ovog korisnog tereta, izmijeniti ga i proslijediti sljedećem čvoru u svojoj aplikaciji.

Čvor funkcije u ovom tijeku prima poruku od IoT čvora i stavlja je u format koji očekuje Db2 Warehouse. Učitavanje **`msg.payload`** za čvor dashDB mora sadržavati vrijednost za svaki stupac u vašoj tablici. Da biste osigurali da vrijednost postoji za svaki stupac, otvorite funkcijski čvor i unesite sljedeći kôd u funkcijsko polje funkcijskog čvora. Ovaj kôd pretvara dolaznu IoT poruku u poruku koju očekuje Db2 Warehouse:

```
<pre> // Format Sensor Data for Db2 Warehouse
msg.payload = {
SENSORID : msg.deviceId,
TEMPERATURE : msg.payload.d.temperature,
HUMIDITY : msg.payload.d.humidity,
PRESSURE : msg.payload.d.pressure,
```

```
TIMESENT : 'TIMESTAMP'
};
return msg;</pre>
```

1. Povucite drugi čvor za otklanjanje pogrešaka u radni prostor i povežite ga s desne strane čvora funkcije.
2. Postavite aplikaciju i provjerite je li izlaz iz vašeg funkcijskog čvora ispravan ispitivanjem izlaza korisnog tereta na kartici za uklanjanje pogrešaka.
3. Nakon što provjerite jesu li podaci pravilno formatirani, spremite ih u bazu podataka: pronađite izlazni čvor dashDB (pohranu) i spojite ga s desne strane čvora funkcije. Napomena: Dvije vrste čvorova dashDB izgledaju slično. Svakako odaberite izlazni čvor koji ima samo jedan konektor na lijevoj strani.
4. Uredite čvor dashDB odabirom usluge baze podataka s popisa i upisivanjem **SENSEDATA** kao naziva tablice.
5. Pokrenite aplikaciju. Podaci vašeg okoliša pohranjeni su u tablicu SENSEDATA. Svaki redak tablice odgovara dolaznom događaju okoline.

Tok 2: Slanje naredbi na uređaj

Drugi protok ubrizgava test podatke koji se šalju Sense HAT uređaju za kontrolu LED diode. Da biste izgradili drugi tok, trebate sedam čvorova. Četiri čvora za ubrizgavanje povezuju se s funkcijskim čvorom, koji se zauzvrat povezuje s izlaznim čvorom ibmiot i čvorom za otklanjanje pogrešaka.

1. U prostor nakon prvog protoka povucite te čvorove u svoj radni prostor i povežite ih. Napomena: Ovaj drugi tok ne trebate kreirati na zasebnoj kartici. Možete koristiti prazan prostor nakon prvog protoka.
2. Postavite čvor za otklanjanje pogrešaka tako da prikazuje cijeli objekt poruke. Četiri čvora za ubrizgavanje pokreću poruke koje kontroliraju LED iz vaše IBM Cloud aplikacije. Kad kliknete gumb na lijevoj strani čvora za ubrizgavanje, u tok se ubrizgava poruka o temi. Pomoću polja teme možete identificirati vrstu naredbe, alarma ili poruke koju želite poslati. Korisni teret je niz koji se šalje na čvor funkcije. Niz se razlikuje za svaki čvor. Čvorovi za ubrizgavanje izgledaju kao ovaj primjer:

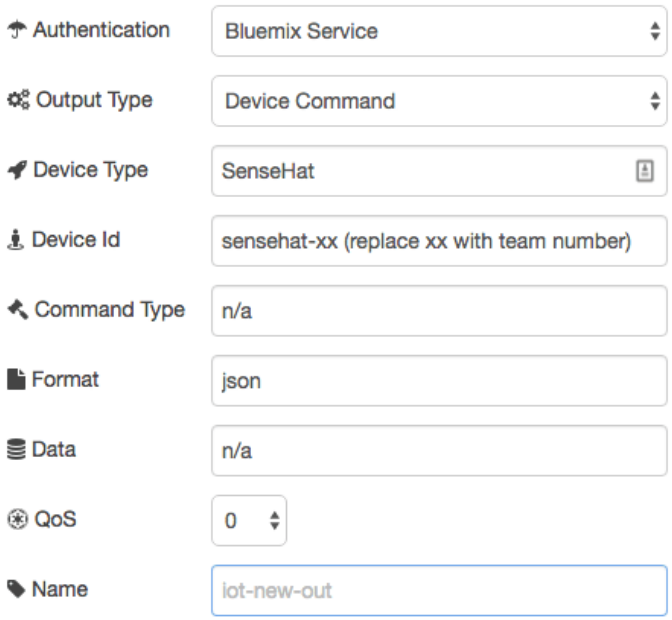
Type	**Payload**	**Topic**	**Name**
string	off	alarm	Turn off LED
string	green	alarm	Green
string	red	alarm	Red
string	Enter any	message	Send Message

message

3. U svoj novi čvor funkcije unesite sljedeći isječak koda. Ovaj kôd stvara odgovarajući JavaScript objekt (d) koji se mora poslati ovisno o vrsti teme. Dolazni msg.payload koristi se kao ulaz za stvaranje objekta. Napomena: Naredba poruke ima još dva parametra, boju i pozadinu. Možete koristiti bilo koju boju za boju i pozadinu.

```
// begin code
msg.eventOrCommandType = msg.topic;
if (msg.topic == "alarm") {
msg.payload={d:{color:msg.payload}};
}
else if (msg.topic == "message") {
msg.payload={d:{color:"navy",
background:"black",
message:msg.payload}};
}
else
msg = null;
return msg;
// end code
```

4. Konfigurirajte izlazni čvor ibmiot. Konfiguracija ovog čvora je poput ulaznog čvora ibmiot.



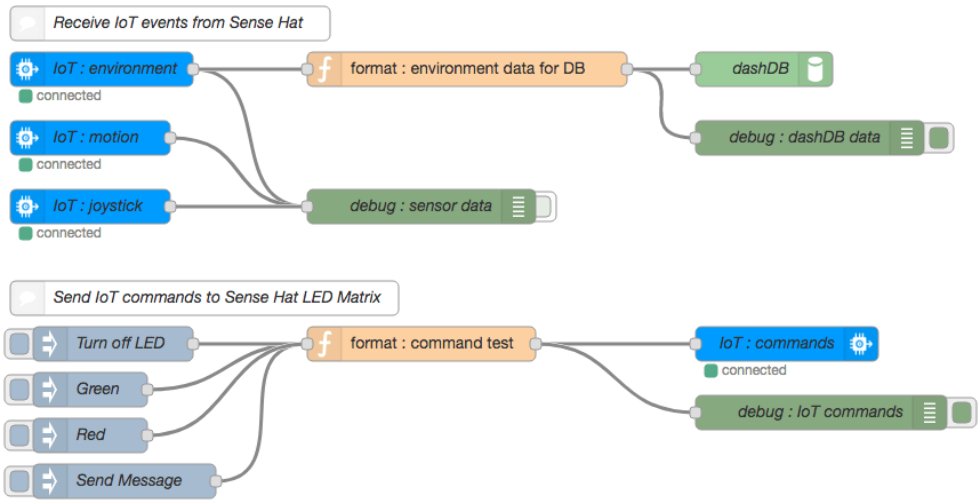
- Vrsta izlaza u ovom je slučaju naredba uređaja za razliku od događaja uređaja. Uređaj šaljete naredbu umjesto da s njega primate događaj.

- Vrsta naredbe i sadržaj podataka nalaze se u msg.payloadu prethodnog čvora. Kao takva, ta se polja zanemaruju. Upišite frazu, poput n / a, kako biste naznačili da su polja zanemarena.

IBM Cloud strana ove aplikacije je potpuna.

5. Kliknite **Deploy** da biste pokrenuli aplikaciju. Testirajte protoke i provjerite radi li sve kako se očekuje. Zadatak 8 uključuje nekoliko testova za provjeru koje možete koristiti.

6. Provjerite izgleda li vaša IBM Cloud aplikacija na sljedećem primjeru:

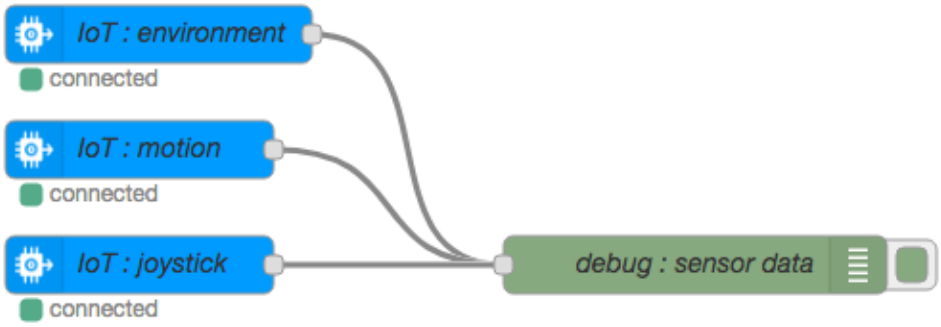


Zadatak 8: Pokrenite I validirajte

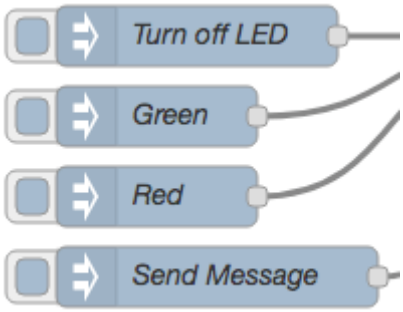
Nakon što stvorite i IBM Cloud i Raspberry Pi Node-RED aplikacije, vrijeme je da pokrenete nekoliko testova kako biste osigurali da vaša aplikacija radi kako se očekuje.

Prije nego što započnete, postavite najnoviju verziju svojih aplikacija. Ako je dugme **Deploy** onemogućen, aplikacija se pokrenuta.

1. U aplikaciji IBM Cloud, koristite čvor za uklanjanje pogrešaka da biste provjerili jesu li sve vrste poruka - okruženje, kretanje i navigacijska palica - poslane u IBM Cloud. Na čvoru za otklanjanje pogrešaka postavite prekidač na isključen i pogledajte podatke na kartici za otklanjanje pogrešaka. Svaki primljeni događaj ima pridruženi typeType. Provjerite vidite li eventType kao dio svake poruke. Ako ne vidite eventType, pobrinite se da je čvor za uklanjanje pogrešaka postavljen tako da prikazuje cijeli objekt poruke. Napomena: Da biste vidjeli događaje na joysticku, morate pomaknuti maleni joystick na SENS HAT.



2. U aplikaciji IBM Cloud koristite čvorove za ubrizgavanje kako biste provjerili reagira li LED senzora HAT kako se očekuje kada pritisnete gumbe za ubrizgavanje. Provjerite rade li sve četiri injekcije ispravno.



Ako ne rade ispravno, provjerite izlaz za otklanjanje pogrešaka iz funkcijskog čvora koji formatira podatke za Sense HAT. U izlaznim podacima provjeravate je li **`eventOrCommandType`** postavljen na ispravnu vrstu naredbe: alarm ili poruka. Također provjerite je li **`payload`** tačan.

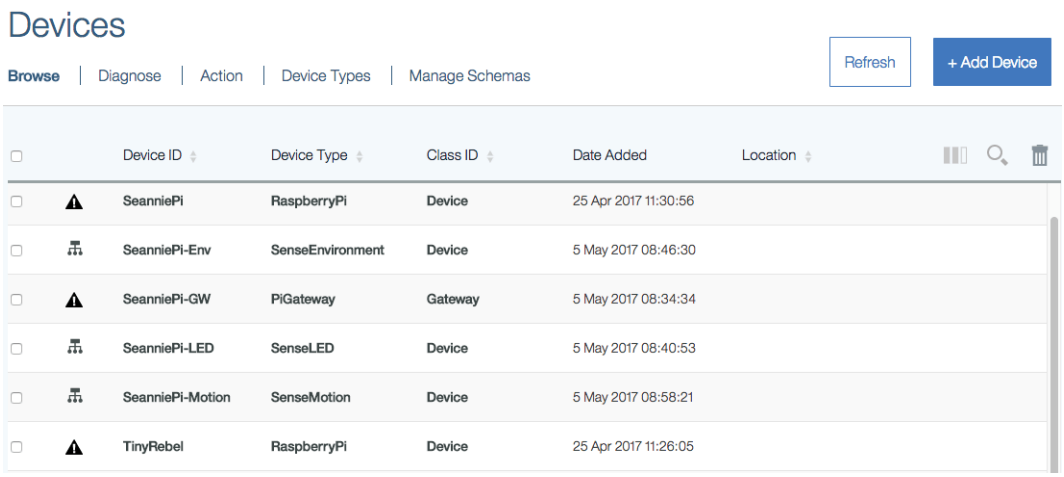
- Primjer naredbe alarma:

```
payload: object
d: object
color: "navy"
```

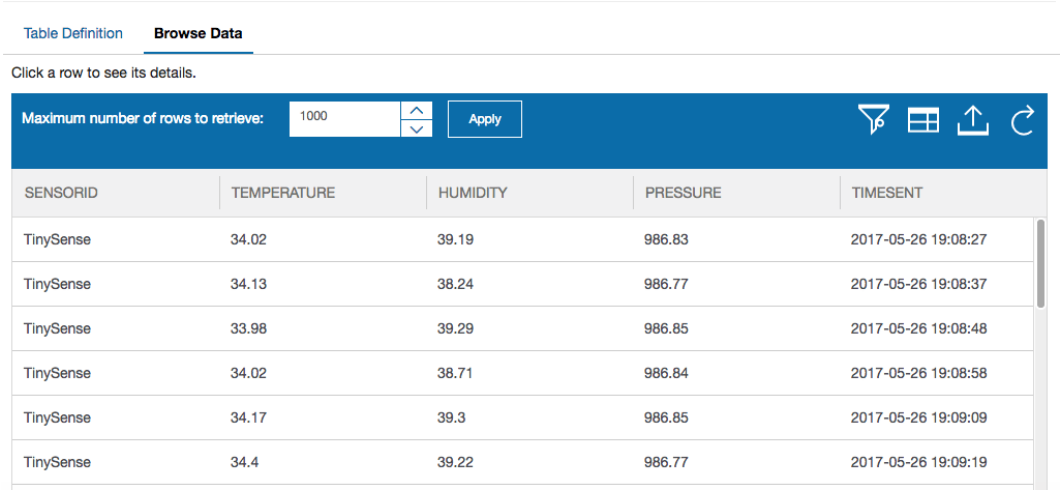
- Primjer naredbe za poruku:

```
payload: object
d: object
color: "navy"
background: "black"
```

3. Sjetimo se da ste karticu preglednika ostavili otvorenu za stranicu IBM Watson IoT Platform Devices. Prebacite se na tu karticu i pregledajte svoj novi uređaj, sensehat-xx tipa SenseHat. Podsjećanja radi, nikada niste stvorili ovaj uređaj ili vrstu uređaja. Za vas ih je stvorio pristupnik Raspberry Pi. Ako niste ostavili karticu preglednika otvorenom, možete je ponovo otvoriti sa svoje nadzorne ploče IBM Cloud. Ako ne vidite svoj novi uređaj, možda ćete trebati osvježiti stranicu.



4. Prebacite se na karticu preglednika koja prikazuje vašu stranicu Db2 Warehouse: Tablice. Ako niste ostavili tu karticu preglednika otvorenom, možete je ponovo otvoriti sa svoje nadzorne ploče IBM Cloud. Kliknite **Browse Data** i pogledajte retke podataka okoline koji se dodaju u vašu tablicu.



5. Ako u tablici ne vidite nijedan redak podataka, provjerite izlaz za otklanjanje pogrešaka iz funkcijskog čvora koji formatira podatke za Db2 Warehouse. U izlaznim podacima provjerite izgleda li korisni teret ovako:

```
Object
SENSORID: "sensehat-xx"
TEMPERATURE: 36.34
HUMIDITY: 34.74
PRESSURE: 991.11
TIMESENT: "TIMESTAMP"
```

Što je sljedeće

Definirali ste IoT uređaje za uslugu Watson IoT Platform i stvorili ste uslugu Db2 Warehouse on Cloud i tablicu Db2 Warehouse za podatke o okolišu. Zatim ste stvorili

aplikacijski prostor IBM Cloud Node-RED, protoci Raspberry Pi Node-RED i IBM Cloud Node-RED prije nego što ste potvrdili svoj rad.

Čestitamo.

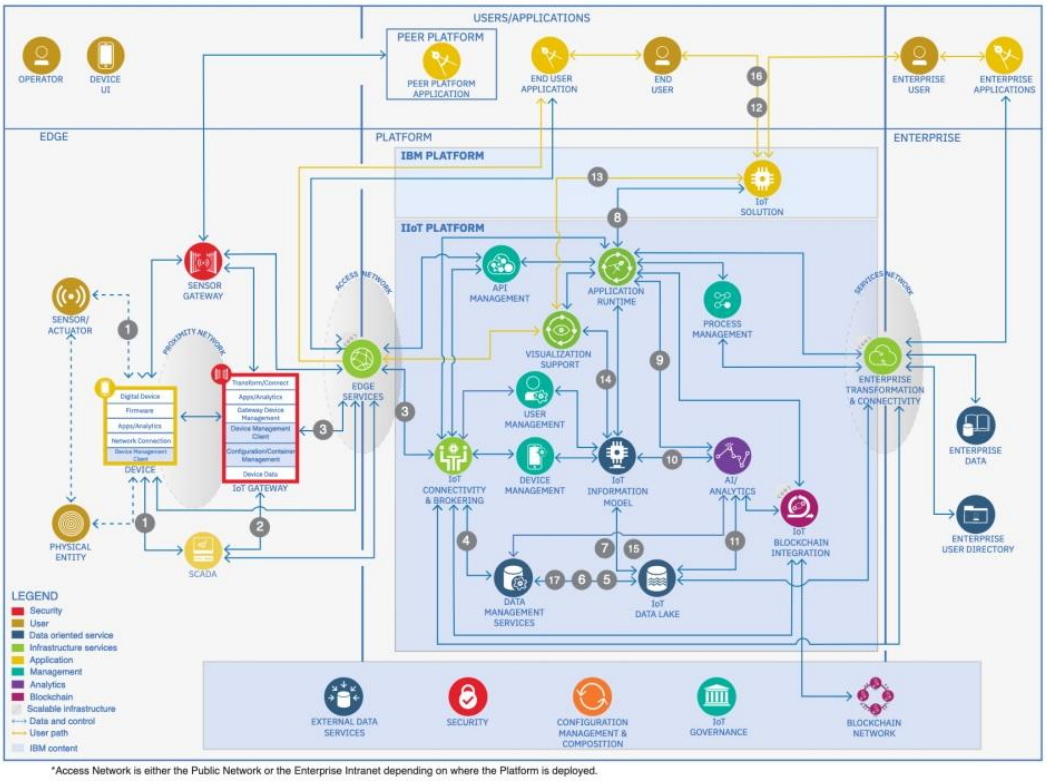
IBM Referenta arhitektura IoT aplikacija

Referentna arhitektura Interneta stvari (IoT) definira IBM-ov pristup IoT rješenjima. Takva rješenja koriste informacije s uređaja, ljudi i aplikacija s uslugama i sustavima u oblaku ili na lokaciji za stvaranje uvida i vrijednosti.

Središte referentne arhitekture je IBM Watson IoT ™ platforma. Tu platformu proširuju IBM, nezavisne tehnologije i tehnologije otvorenog koda kako bi se osigurale mogućnosti platforme Industrial Internet of Things (IIoT), kako je definirana Referentnom arhitekturom IIoT Industrial Consortiuma. Namjera je definirati logičku arhitekturu koja ostaje dosljedna čak i kad se fizičke sposobnosti mijenjaju.

Ova referentna arhitektura polazna je tačka za projekte i za rješenja koja se temelje na Watson IoT platformi. Primjeri uključuju IoT za izgradnju uvida i Industrie 4.0.

Prikaz: IoT referentna arhitektura



Korak 1.

Podaci senzora prelaze iz senzora u ili oko zgrade do nadzornog sustava upravljanja i prikupljanja podataka (SCADA) koji kontrolira procesnu opremu. Senzor je povezan sa SCADA sustavom pomoću protokola bežičnog ili žičanog uređaja, kao što je RS 485.

Korak 2.

SCADA sistem izlaže podatke vanjskom svijetu pomoću protokola Operativne tehnologije (OT), kao što je Modbus TCP. Ako je potrebno, podaci senzora mogu se pretvoriti u drugi format prije prijenosa. Podaci o energiji prenose se na IoT pristupnik čitanjem preslikanih podataka i OT protokola.

Korak 3.

Ako je potrebno, IoT pristupnik filtrira podatke senzora, poput vremenskog intervala, agregiranja i usrednjavanja, i pretvara ih u format koji IoT rješenju treba. IoT pristupnik uspostavlja sigurnu vezu s IoT platformom pomoću TLS-a i prenosi energetske podatke na platformu pomoću MQ Telemetry Transport (MQTT).

Korak 4.

Usluga za upravljanje podacima prikupljaju sirove podatke ulaznog senzora radi odlaganja.

Korak 5.

Sirovi podaci pohranjuju se u podatkovno jezero u formatu u kojem su primljeni.

Korak 6.

Na temelju konfiguracije, podaci se povremeno reorganiziraju u podatkovnom jezeru kako bi podržali analitiku.

Korak 7.

Model informacija koristi se za pružanje konteksta za mjesto uređaja unutar poduzeća. Taj se kontekst koristi za uspostavljanje tablica unutar IBM Db2® za organiziranje podataka.

Korak 8.

Izvršavanje analitičkog modela povremeno se pokreće za procjenu ažuriranih podataka uređaja. Rezultati se pohranjuju u podatkovno jezero. Model izvršenja također se može automatski pokrenuti na temelju događaja primljenih u Internet Open Trading Protocol (IOTP).

Korak 9.

Izvršenje analitičkog modela povremeno se pokreće za procjenu ažuriranih podataka uređaja. Rezultati se pohranjuju u podatkovno jezero.

Korak 10.

Analitički model koristi informacijski model za pružanje konteksta za predviđanja imovine; na primjer, očekivano vrijeme do neuspjeha.

Korak 11.

Rezultati predviđanja imovine pohranjuju se u podatkovnom jezeru.

Korak 12.

Korisnik IoT rješenja pristupa korisničkom sučelju radi pregleda podataka o imovini i srodnih rezultata analitike.

Korak 13.

Korisnik IoT rješenja pristupa korisničkom sučelju radi pregleda podataka o imovini i srodnih rezultata analitike.

Korak 14.

Model informacija koristi se za pružanje konteksta za mjesto imovine i uređaja unutar poduzeća i odgovarajuće podatke.

Korak 15

Kontekst informacijskog modela koristi se za pristup informacijama u podatkovnom jezeru koje će se prikazati za uređaje u kontekstu.

Korak 16

Korisnik IoT rješenja vidi da je sredstvo bilo ili će biti izvan tolerancije i šalje tehničara za održavanje da istraži problem. Tehničar za održavanje otkrije da dio opreme otkazuje i rješava problem.

Korak 17

Na temelju konfiguracije, podaci se povremeno premještaju iz Db2 u spremište predmeta kao dio dugoročnog postupka arhiviranja podataka

IT Arhitekt asistent

Predlošci dijagrama arhitekture omogućuju vam lako stvaranje vlastitih arhitektura pomoću jednostavnih ikona za predstavljanje komponenata arhitekture. Možete

započeti s postojećim uzorkom, a zatim ga prilagoditi svom okruženju ili izraditi vlastiti uzorak ispočetka koristeći bilo koju kombinaciju komponenata.

To možete probati na slijedećem linku:

https://www.ibm.com/cloud/architecture/architectures/edit

ALDI INICIJATIVA ZA INOVATIVNI TRENING

Panorama b.b. 73 000 Goražde

Bosna i Hercegovina

INTERNET OF THINGS

IOT SIGURNOST

AITI-IOT-001-180-05

IoT sigurnost

Povezivanje svih stvari u Internet of Things

AITI

Skill Accelerator

Follow us at @UAITLab

IoT sigurnost

Povezivanje svih stvari u Internet of Things

Početkom 20 stoljeća nafta je bila glavni motor do tada neviđenog progresa i napredka širom svijeta. Sto godina kasnije nafti se bliži kraj (kako zbog ograničenih resursa tako i zvog negativnog uticaja na okoliš) mjesto ključnog resursa na kojem se zasniva razvoj sve više preuzimaju podaci koji su glavni motor četvrte industrijske revolucija (Industrija 4.0).

U predhodnom poglavlju imali ste prilike kako bi napravili dobru strategiju. I kao što ste mogli primjetiti, korištenje ovih alata skoro pa bezvrijedno bez odgovarajućih, tačnih i relevantnih podataka.

Kako bi bili u mogućnosti da skoristite puni potencijal podataka u ovom poglavlju su obrađene teme koje će vam pomoći da usvojite znanja iz oblasti poslovnog obavještanja (Business Intelligence) čija primjena doprinosi boljem, bržem i efikasnijem donošenju odluka, te će steći vještine rada sa podacima u softverskim platformama za provođenje analitike podataka u poslovne svrhe.

U ovom poglavlju vi će te se moći upoznati sa:

- Osnovama pristupa poslovnog obavlještavanja i novim pristupima korištenja poslovnih podataka u procesu donošenja odluka u organizaciji;
- Osnovama rada sa podacima kako bi mogli iskoristiti njihov puni potencijal za primjenu poslovne analike u upravljačkim procesima;
- Mogućnostima koje nude softverkse platfome Tableau i Power BI, dvije trenutno najbolje softverske platforme za poslovnu analitiku i Business intelligence za mala i srednja preduzeća/organizacije.

Znanje sa kom se možete upoznati u ovom poglavlju sigurno će vam olakšati napore na razvoju vaših strateških ideja. Međutim, oni vam takođe mogu biti od izuzetne koristi kada budete razvijali vaše prijedloge projekata putem vi vaše strateške ideje razrađujete u detaljne planove akcije.

Poslovna analitika u doba podataka postaje sve važniji alat koji se primjenjuje u poslovanju, zato ne gubimo vrijeme i krenimo da se upoznamo sa ovom jako zanimljivom temom.

1. Osnove IoT sigurnosti

Uvod o sigurnosti operativnih tehnologija (OT);

Uvod o sigurnosti operativnih tehnologija (OT)

Da bismo bolje razumjeli trenutnu situaciju u industrijskim okruženjima, važno je razlikovati pretpostavke od stvarnosti.

Nekoliko tema u informacijskoj tehnologiji potaknuti više straha, neizvjesnosti ili sumnje od cyber sigurnosti.

Više nego u većini drugih sektora, incidenti kibernetičke sigurnosti u industrijskim okruženjima mogu rezultirati fizičkim posljedicama koje mogu uzrokovati prijetnje ljudskim životima, kao i štetu na opremi, infrastrukturi i okolišu.

Iako sigurno postoje tradicionalne prijetnje sigurnosti povezane s IT-om u industrijskim okruženjima, to su fizičke manifestacije I utjecaji sigurnosnih incidenata u OT-u koji plijene pozornost medija i izazivaju široko utemeljeno brigu javnosti.

Mnoge sigurnosne politike i postojeći postupci ublažavanja ostali su bez pažnje; međutim, ako pravilno provedeni, mogli su u potpunosti spriječiti ili eventualno zaustaviti napade.

Osim fizičke štete, operativni su se prekidi dogodili i u okružjima za zabranu zbog incidenata u cyber-sigurnosti. Na primjer, 2000. godine, sustav za kontrolu kanalizacije iz Maroochy Shirea u Queenslandu u Australiji pristupilo se na daljinu i pušteno je 800.000 litara kanalizacije u okolne plovne putove. U 2015. kontrolni sustavi ukrajinskog operatora distribucije električne energije Kijev Oblenergo imali su pristup na daljinu napadači, uzrokujući prekid u trajanju od nekoliko sati koji je rezultirao danima degradacije usluga za tisuće kupaca. U oba slučaja, poznate tehnike ublažavanja mogu primijenjeni su za ranije otkrivanje napada ili blokiranje mogućnosti otmice proizvodnje sustavi i utječu na uslugu.

Istorijski gledano, napadači su bili vješti pojedinci s dubokim poznavanjem tehnologije I sistema koje su napadali. Međutim, kako je tehnologija napredovala, alati su bili stvorena kako bi se napadi učinili mnogo lakšima za izvođenje. Da bi dodatno zakomplicirali stvari, ovo alati su postali šire dostupni i lakše dostupni.

Komplicirajući problem je u tome da su mnogi naslijeđeni protokoli koji se koriste u IoT okruženjima stari su desetljećima, i nije se mislilo na sigurnost kad su prvi put razvijeni. Ovo znači da napadači s ograničenim ili nikakvim tehničkim mogućnostima sada imaju potencijal pokrenuti cyber napad, uvelike povećavajući učestalost napada i ukupnu

prijetnju krajnjim operaterima. Česta je zabluda da napadači uvijek imaju prednost i da krajnjim operaterima nedostaju učinkovite obrambene sposobnosti. Važna prednost za operatora je činjenica da su daleko upoznati sa svojim okruženjem i da imaju bolje razumijevanje njihovih procesa, a time može iskoristiti više tehnologija I mogućnosti obrane svojih mreža od napada. To je presudno kao što će i mreže i dalje se suočavati sa stalno razvijajućim se i promjenjivim metodama napada koje će biti sve više teško obraniti i odgovoriti na njih.

U Hrvatskoj su korištene komunikacijske mreže, lokalne i zemljopisno raspršene industrijska okruženja desetljećima. Na primjer, daljinski nadzor trafostanica i komunikacije između poluautonomnih sustava u proizvodnji su dugogodišnji primjeri takvih OT mreža. Ovi komunikacijski sustavi specifični za OT su obično samostalni i fizički izolirani od tradicionalnog informatičkog poduzeća mreže u istim tvrtkama. Iako slijedi tradicionalnu logiku „sigurnosti kroz nejasnoće“, ovaj oblik mrežne kompartmentalizacije doveo je do neovisnog razvoja IT i OT mreža, s međusobnim vezama između okruženja strogo odvojeno i nadzirano.

Izolacija između industrijskih mreža i tradicionalnih IT poslovnih mreža ima nazivan je "zračnim jazom", što sugerira da između njih nema veza.

Iako postoje primjeri takve ekstremne izolacije u nekim industrijama, to zapravo nije točan opis većine IoT mreža danas. Široko govoreći, postoji različita količina međusobne povezanosti između OT i IT mrežnih okruženja, i mnoga međuovisnosti između njih dvoje utječu na razinu međusobne povezanosti.

Uobičajeni izazovi sigurnosti operativnih tehnologija

Sigurnosni izazovi s kojima se IoT susreće nisu nimalo novi i nisu ograničeni na određene industrijska okruženja.

Nekoliko je uobičajenih izazova sigurnosti sa kojima se se suočava IoT.

Erozija mrežne arhitekture

Dva glavna izazova u osiguranju industrijskog okruženja bili su početni dizajn i trajno održavanje. Početni izazovi u dizajnu proizašli su iz koncepta koji je bio zasnovan na tome da da su mreže sigurne zbog fizičkog odvajanja od poduzeća s minimalnim ili nikakvimpovezanost s vanjskim svijetom i pretpostavka da napadačima nedostaje dovoljno znanje za izvođenje sigurnosnih napada. U mnogim je slučajevima početni dizajn mreže izgledao je dobro I često je slijedo dobro definirane najbolje industrijske prakse i standarde, poput Purdueov modela za hijerarhiju upravljanja.

Izazov je i najveća prijetnja sigurnosti mreže je standard ili najbolje prakse koje se ili se krivo razumiju ili je mreža loše održavana. Zapravo, iz perspektive sigurnosnog dizajna, bolje je znati da su komunikacijski putovi nesigurni nego ne znati stvarne putove komunikacije. to je uobičajenije da se s vremenom ono što je možda za početak bilo solidan dizajn nagriza kroz ad hoc ažuriranja i pojedinačne promjene hardvera i uređaja bez razmatranje šireg utjecaja mreže.

Ova vrsta organskog rasta dovela je do pogrešne proračune širenja mreža i uvođenje bežične komunikacije u samostalni način, bez razmatranja utjecaja na izvorni sigurnosni dizajn.

Ova nekontrolirana ili slabo kontrolirana evolucija OT mreže su, u mnogim slučajevima, s vremenom je doveo do slabe ili neodgovarajuće sigurnosti mreže i informatičkog sistema.

Postoji široka raznolikost dizajna zaštićenih mreža unutar različitih industrija.

Na primjer, elektroenergetska poduzeća imaju snažnu istoriju korištenja modernih tehnologija za operativne aktivnosti, au Sjevernoj Americi postoje regulatorni zahtjevi od regulatornih tijela, poput Sjevernoameričke korporacije za električnu pouzdanost (NERC-ova) Zaštita kritične infrastrukture (CIP), za implementaciju sigurne mrežne povezanosti i kontrole pomoću razumno propisane radnje.

Suprotno tome, u drugim industrijama često ih nema zakonskih zahtjeva ili politika poštivanja, što je rezultiralo širokim rasprostranjenjem razlike u sigurnosnim mogućnostima.

U mnogim se industrijama upravljački sustavi sastoje od paketa, klizača ili komponenata koje su samostalni i mogu se integrirati kao poluautonomni dijelovi mreže.

Ovi paketi ne moraju biti potpuno ili čvrsto integrirani u cjelokupni sistem upravljanja, alata za upravljanje mrežom ili sigurnosnih aplikacija što rezultira potencijalnim rizikom.

Prožimajući naslijeđeni sistemi

Zbog statičke prirode i dugog životnog ciklusa opreme u industrijskim okruženjima, mnogi operativni sistemi mogu se smatrati naslijeđenim sistemima.

U mnogim slučajevima, naslijeđene komponente nisu ograničeni na izolirane mrežne segmente, ali su sada konsolidirani u IT operativno okruženje. Iz sigurnosne perspektive, ovo je potencijalno opasno jer mnogi uređaji mogu imati povijesne ranjivosti ili slabosti koje nisu bile zakrpe i ažuriraju, ili može biti da zakrpe nisu dostupne ni zbog starosti od

oprema.

Osim krajnjih točaka, komunikacijska infrastruktura i zajedničko centralizirano računanje resursi se često ne grade u skladu sa suvremenim standardima. Zapravo, njihove komunikacijske metode i protokoli mogu biti stare generacije i moraju biti interoperabilni s njima najstariji operativni entitet u komunikacijskoj putanji. To uključuje prekidače, usmjerivače, vatrozidi, bežične pristupne točke, poslužitelji, sistemi za daljinski pristup, upravljanje zakrpama I alati za upravljanje mrežom. Sve ove mogu imati ranjive točke koje se mogu iskoristiti i moraju biti zaštićene.

Nesigurni operativni protokoli

Mnogi su protokoli industrijske kontrole, posebno oni koji su serijski utemeljeni dizajniran bez inherentnih jakih sigurnosnih zahtjeva. Nadalje, njihov rad često bio unutar pretpostavljene sigurne mreže. Pored svih svojstvenih slabosti ili ranjivosti, njihovo operativno okruženje možda nije dizajnirano s osiguranim na vodeći računa o kontroli pristupa.

Nesigurnost uređaja

Osim komunikacijskih protokola koji se koriste i instalacijske baze sustava naslijeđeni sustavi, upravljački i komunikacijski elementi sami imaju istoriju ranjivosti. Prije 2010. Godine sigurnosna zajednica obraćala je malo pažnje na industrijske račune i kao rezultat toga,

Da biste razumjeli prirodu nesigurnosti uređaja, važno je pregledati istoriju koje su ranjivosti otkrivene i koje su vrste uređaja pogođene.

Ovisnost o vanjskim dobavljačima

Iako moderna informatička okruženja možda prepuštaju poslovno poslovanje ili odstupaju određene funkcije obrade ili pohrane u Cloud.

Međutim, ta razina ovisnosti o dobavljačima kod nekih nije rijetka industrijski prostori. direktni pristup na zahtjev i kritični sustavi na podu postrojenja ili na terenu jesu ponekad upisani izravno u ugovore ili su potrebni za valjana jamstva za proizvode.

Sigurnosno znanje

U industrijskom operativnom prostoru, tehničko ulaganje prvenstveno je u povezanost i izračunati. Vidjelo je daleko manje ulaganja u sigurnost u odnosu na IT kolegu.

Prema istraživačkoj tvrtki Infonetics, tržište industrijskog vatrozida u 2015. godini bilo je samo otprilike 4% veličine cjelokupnog tržišta vatrozida.

IoT sigurnosi izazovi i zabrinutosti

IoT je atraktivan i to je ono što potrošače potiče da ih usvoje, čak i prije nego što budu spremni, pa čak i prije nego što sami uređaji budu u potpunosti opremljeni sigurnosnim standardima.

Budući da ova tehnologija još nije sazrela, još uvijek postoje mnogi izazovi koje treba prevladati - kako od strane proizvođača, tako i od korisnika. Svi oni uglavnom proizlaze iz:

- Nedostatak korisničkog znanja
- Nedosljedni proizvodni standardi
- Loše održavanje i ažuriranja

Sve ove opće kategorije izazova sadrže specifičnije IoT probleme i ranjivosti. Obratimo se sada onima koji prijete.

Od otmice IoT uređaja preko potencijalnih invazija na kuće do opasnosti od nevaljalih uređaja, ovde smo naveli neke od trenutno najzastupljenijih izazova I zabrinutosti o kojima treba da vodite računa prilikom razvoja vašeg IoT projekta.

Izazovi

1. Sigurnosno ograničeni uređaji

Mnogi IoT uređaji imaju ograničene količine prostora za pohranu, memoriju i mogućnosti obrade i često moraju biti u mogućnosti raditi s manjom snagom, na primjer, kada rade na baterije.

Sigurnosni pristupi koji se u velikoj mjeri oslanjaju na šifriranje nisu pogodni za ove ograničene uređaje jer nisu sposobni izvršiti složeno šifriranje i dešifriranje dovoljno brzo da bi mogli sigurno prenositi podatke u stvarnom vremenu.

Ovi su uređaji često ranjivi na napade bočnih kanala, poput napada na analizu snage, koji se mogu koristiti za obrnuti inženjering ovih algoritama. Umjesto toga, ograničeni uređaji obično koriste samo brze, lagane algoritme šifriranja.

IoT sistemi trebali bi koristiti više slojeva obrane, na primjer, odvajanje uređaja na zasebne mreže i korištenje vatrozida, kako bi nadoknadili ta ograničenja uređaja.

2. Odobravanje i provjera autentičnost uređaja

S toliko mnogo uređaja koji nude potencijalne tačke ulaska u IoT sistem, provjera autentičnosti i autorizacija uređaja presudna je za zaštitu IoT sustava.

Uređaji moraju utvrditi svoj identitet prije nego što mogu pristupiti pristupnicima i uslugama i aplikacijama uzvodno. Međutim, postoje mnogi IoT uređaji koji propadaju kada je u pitanju autentifikacija uređaja, na primjer, pomoću slabe osnovne autentifikacije lozinke ili pomoću lozinki nepromijenjenih u odnosu na zadane vrijednosti.

Usvajanje IoT platforme koja prema zadanim postavkama pruža sigurnost pomaže u rješavanju ovih problema, na primjer omogućavanjem dvofaktorske autentifikacije (2FA) i prisilnom upotrebom jakih lozinki ili certifikata. IoT platforme također pružaju usluge autorizacije uređaja koje se koriste za određivanje usluga, aplikacija ili resursa kojima svaki uređaj ima pristup u cijelom sustavu.

3. Upravljanje ažuriranjima uređaja

Primjena ažuriranja, uključujući sigurnosne zakrpe, na firmware ili softver koji se izvodi na IoT uređajima i pristupnicima predstavlja niz izazova. Na primjer, trebate pratiti koja su ažuriranja dostupna, primijeniti ih sinkronizirano u distribuiranim okruženjima s heterogenim uređajima koji komuniciraju kroz niz različitih mrežnih protokola. Morate primijeniti gracioznu strategiju povratka u slučaju da ažuriranje ne uspije.

Ne podržavaju svi uređaji bežična ažuriranja ili ažuriranja bez zastoja, pa će uređajima možda trebati fizički pristupiti ili ih privremeno izvući iz proizvodnje da bi primijenili ažuriranja. Također, ažuriranja možda neće biti dostupna za sve uređaje, posebno za starije uređaje ili one uređaje koje njihov proizvođač više ne podržava.

Čak i kada su dostupna ažuriranja, vlasnici uređaja mogu se odbiti od primjene ažuriranja, pa je važno zadržati kompatibilnost s unatrag. Kao dio upravljanja uređajem, morate pratiti verzije koje su postavljene na svakom uređaju i koji su uređaji kandidati za umirovljenje nakon što ažuriranja više nisu dostupna.

Sistemi upravitelja uređaja često podržavaju automatsko potiskivanje ažuriranja na uređaje, kao i upravljanje vraćanjima u slučaju da postupak ažuriranja ne uspije. Oni također mogu pomoći u osiguranju primjene samo legitimnih ažuriranja, na primjer upotrebom digitalnog potpisivanja.

4. Sigurna komunikacija

Nakon što se osiguraju sami uređaji, sljedeći je IoT sigurnosni izazov osigurati sigurnu komunikaciju putem mreže između uređaja i usluga u oblaku ili aplikacija.

Mnogi IoT uređaji ne kriptiraju poruke prije slanja putem mreže. Međutim, najbolja je praksa korištenje šifriranja prijevoza i usvajanje standarda poput TLS-a. Korištenje zasebnih mreža za izoliranje uređaja također pomaže u uspostavljanju sigurne, privatne komunikacije, tako da preneseni podaci ostaju povjerljivi. Uobičajene mjere uključuju upotrebu vatrozida, ograničavanje fizičkog pristupa gateway uređajima, upotrebu nasumično generirane jednokratne lozinke i isključivanje značajki OS-a koje uređaj ne zahtijeva.

5. Osiguranje privatnosti i integriteta podataka

Također je važno da, gdje god podaci završe nakon što se prenesu mrežom, oni se sigurno pohrane i obrade. Implementacija privatnosti podataka uključuje uređivanje ili anonimiziranje osjetljivih podataka prije nego što se pohrane ili korištenje odvajanja podataka za razdvajanje podataka koji mogu osobno identificirati podatke IoT podataka. Podaci koji više nisu potrebni trebaju se zbrinjavati na siguran način, a ako se podaci pohranjuju, važan je izazov i poštivanje zakonskih i regulatornih okvira. Povećan je interes za razvojem sustava koji omogućuju federalno strojno učenje, pri čemu podaci ostaju lokalni na uređaju, a rad na strojnom učenju događa se na rubu, a samo se učenja / uvidi dijele s oblakom. Suština takvih sustava je da algoritam treba doći do podataka umjesto uobičajenih metoda gdje svi podaci odlaze u algoritam.

Osiguravanje integriteta podataka, što može uključivati upotrebu kontrolnih suma ili digitalnih potpisa kako bi se osiguralo da podaci nisu promijenjeni. Blockchain - kao decentralizirana distribuirana knjiga za IoT podatke - nudi skalabilan i elastičan pristup za osiguravanje integriteta IoT podataka.

6. Sigurne web, mobilne i Cloud aplikacije

Web, mobilne i cloud aplikacije i usluge koriste se za upravljanje, pristup i obradu IoT uređaja i podataka, tako da ih također moraju osigurati kao dio višeslojnog pristupa IoT sigurnosti. Treba se pridržavati svih standardnih praksi zaštite mobilnih i web aplikacija.

Kada razvijate IoT aplikacije, primijenite sigurne inženjerske prakse kako biste izbjegli ranjivosti poput OWASP top 10 ranjivosti. Baš kao i uređaji, i aplikacije bi trebale podržavati sigurnu provjeru autentičnosti, kako za same aplikacije, tako i za korisnike aplikacija, pružajući opcije poput 2FA i mogućnosti sigurnog oporavka lozinke.

7. Osiguranje visoke dostupnosti

Kako se u svakodnevnom životu više oslanjamo na IoT, programeri IoT-a moraju uzeti u obzir dostupnost IoT podataka i weba i mobilnih aplikacija koje se oslanjaju na te podatke, kao i naš pristup fizičkim stvarima kojima upravljaju IoT sustavi . Potencijal za prekide kao rezultat prekida veze ili kvara uređaja ili koji nastaju kao rezultat napada poput napada uskraćivanja usluge više je od neugodnosti. U nekim aplikacijama utjecaj nedostatka dostupnosti mogao bi značiti gubitak prihoda, štetu na opremi ili čak gubitak života.

Na primjer, u povezanim gradovima IoT infrastruktura odgovorna je za osnovne usluge kao što je kontrola prometa, a u zdravstvu IoT uređaji uključuju pacemakere i inzulinske pumpe. Da bi se osigurala visoka dostupnost, IoT uređaji moraju biti zaštićeni od cyber napada, kao i od fizičkog neovlaštenog miješanja. IoT sustavi moraju uključivati suvišnost kako bi se eliminirale pojedinačne točke kvara, a također bi trebali biti dizajnirani da budu otporni i otporni na kvarove, tako da se mogu brzo prilagoditi i oporaviti kad se pojave problemi. Budući da se većina IoT sustava distribuira u prirodi, važno je imati na umu CAP teorem (distribuirani računalni sustav može imati najviše dva svojstva zbog velike dostupnosti, dosljednosti i tolerancije na mrežnu particiju).

8. Spriječavanje incidenata otkrivanjem ranjivosti

Unatoč najboljim naporima, sigurnosne ranjivosti i proboji su neizbježni.

Kako znati je li vaš IoT sistem ugrožen?

U IoT sistemima velikih razmjera, složenost sistema u smislu broja povezanih uređaja i raznolikosti uključenih uređaja, aplikacija, usluga i komunikacijskih protokola može otežati prepoznavanje trenutka kada se dogodio incident. Strategije za otkrivanje ranjivosti i kršenja uključuju praćenje mrežnih komunikacija i evidencija aktivnosti zbog nepravilnosti, uključivanje u testiranje prodora i etičko hakiranje radi otkrivanja ranjivosti te primjenu sigurnosnih podataka i analitike za identificiranje i obavještavanje o incidentima.

9. Upravljanje ranjivostima

Složenost IoT sistema također predstavlja izazov za procjenu posljedica ranjivosti ili opsega kršenja kako bi se upravljalo njegovim utjecajem. Izazovi uključuju identificiranje na koje su uređaje to utjecalo, kojim podacima ili uslugama je pristupljeno ili su ugroženi

i koji su to korisnici pogođeni, a zatim poduzimanje neposrednih radnji za rješavanje situacije.

Upravitelji uređaja vode registar uređaja koji se može koristiti za privremeno onemogućavanje ili izoliranje pogođenih uređaja dok se ne mogu zakrpati. Ova je značajka posebno važna za ključne uređaje (kao što su gateway uređaji) kako bi se ograničila njihova potencijalna šteta ili poremećaj, na primjer preplavljivanje sustava lažnim podacima ako su ugroženi. Akcije se mogu automatski primijeniti pomoću mehanizma pravila s pravilima koji se temelje na politikama upravljanja ranjivostima.

10. Predvidite i spriječite sigurnosne probleme

Dugoročni sigurnosni izazov IoT-a je primjena sigurnosnih obavještajnih podataka ne samo za otkrivanje i ublažavanje problema onako kako se javljaju, već i predviđanje i proaktivna zaštita od potencijalnih sigurnosnih prijetnji. Modeliranje prijetnji jedan je od pristupa koji se koristi za predviđanje sigurnosnih problema. Ostali pristupi uključuju primjenu alata za praćenje i analitiku za korelaciju događaja i vizualiziranje odvijanja prijetnji u stvarnom vremenu, kao i primjenu AI za prilagodljivo prilagođavanje sigurnosnih strategija primijenjenih na temelju učinkovitosti prethodnih radnji. Suština je minimizirati ljudsku intervenciju i isprazniti što više rada na algoritme, jer je kontinuirano ručno ispitivanje gotovo nemoguće.

Zabrinutosti

1. Otmica IoT uređaja i Ransomwarea

IoT uređaji koji imaju slabe sigurnosne mjere mogu postati meta ransomwarea - zlonamjernog softvera koji šifrira i blokira pristup osjetljivim datotekama korisnika.

Pravi problem započinje kada haker koji je zarazio uređaj zlonamjernim softverom zahtijeva novac za otkupninu ako žrtva želi vidjeti njihove datoteke otključane.

Zvuči vrlo distopično, ali svejedno je stvarnost - srećom, rijetka stvarnost do sada. Međutim, ovo postaje sve veći trend u podzemnoj hakerskoj sferi.

Ova sigurnosna prijetnja mogla bi staviti u veliki rizik nosivu tehnologiju, uređaje za praćenje zdravstvene zaštite i pametne domove. Uznemirujuća je misao pomisliti na zaključanu kuću ili pametno vozilo koje se ne pokreće dok otkupnina ne bude plaćena.

Ransomware napadi ne mogu samo zaključati korisnike iz IoT uređaja i srodnih platformi, već i potpuno onemogućiti uređaje i ukrasti korisničke podatke.

Brzi porast globalnog broja IoT uređaja učinit će ovo posebno IoT sigurnosno pitanje nepredvidljivim u smislu mogućih permutacija. Međutim, dobra vijest je da, budući da je većina IoT informacija pohranjena u oblaku, ovaj zlonamjerni softver možda neće imati vrijedne podatke za zaključavanje.

2. Nedovoljno testiranje i nedostatak ažuriranja

Jedan od sigurnosnih problema s IoT uređajima jest da se prilikom razvoja IoT projekta često bude neoprezno što se tiče ispravnog testiranja i pružanja pravovremenih ažuriranja softvera.

To je velik problem jer potrošači vjeruju proizvođačima i njihovoj prosudbi te su često uvjereni da su poduzeli sve mjere kako bi osigurali sigurnosne propuste.

No, zbog ubrzanog rasta tržišta IoT, mnogi žure sa svojim projektima i puštanjem svojih proizvoda bez da se mnogo razmišlja o testiranju.

Ponekad su jedina ažuriranja u ponudi za kraća vremenska razdoblja. A budući da je hiperprodukcija uređaja također stvarnost, oni mogu napustiti ova ažuriranja da bi se umjesto toga usredotočili na novu generaciju uređaja i pozivajući ljude da se prebace na njih.

Kao rezultat toga, vaš IoT uređaj s zastarjelim softverom može biti izložen bezbroj napada zlonamjernog softvera i hakera te drugim narušavanjima sigurnosti.

Postoji čak i još jedna zastrašujuća mogućnost: tijekom ažuriranja može doći do zastoja kada uređaj pošalje svoje podatke u Cloud. Tokom ovog duljeg razdoblja i ako vaša veza nije šifrirana, datoteke ažuriranja mogu biti nezaštićene što hakerima otvara vrata.

Redovita automatska ažuriranja od najveće su važnosti za izbjegavanje IoT sigurnosnih problema. Potrebno je da shvatite da je vaša dužnost ažurirati softver uređaja čim se izlože ranjivosti i određeni napadi zlonamjernog softvera postanu rašireni.

3. Kućne invazije

Vjerojatno najneugodniji scenarij IoT sigurnosnih problema su upadi u kuću ili invazije na kuće jer oni zamagljuju granicu između virtualnog i fizičkog svijeta i dovode korisnike u vrlo stvarnu, opipljivu opasnost.

Uređaji Interneta stvari postaju dijelom sve većeg broja domova koji su rodili koncept "pametnih domova".

Ova automatizacija kuće dolazi s velikom prijetnjom jer nesigurni uređaji, sa lošim obrambenim mehanizmima, mogu emitirati IP adrese. Takozvana pretraživanja Shodan mogu hakerima omogućiti lociranje adrese korisnika uređaja.

Način da se spriječi ovo kršenje IoT sigurnosti jest povezivanjem putem VPN-ova i osiguravanjem vaših vjerodajnica za prijavu - o čemu ćemo razgovarati kasnije u članku.

4. Financijski kriminal pokrenut IoT-om

Tvrtke za elektroničko plaćanje koje primjenjuju Internet stvari mogu očekivati da će doći do porasta financijskog kriminala i sintetičkih prijevara s identitetom.

Neke od tih tvrtki eksperimentiraju s umjetnom inteligencijom i Machine learning, dok će mnoge od njih uskoro morati prepoznati važnost integriranja informacija na različitim poslovnim razinama.

To je osiguravanje pravovremenog otkrivanja obrazaca prijevare i njihovih složenih signala pomoću dubokog učenja.

Sve financijske kompanije suočit će se s izazovom lansiranja ovih novih modela jer imaju problema s usklađenošću i operativnim problemima. Odnosno, osim ako ne poboljšaju strategije životnog ciklusa i upravljanja rizikom koje uključuju rastuću prijetnju proboja IoT sigurnosti.

5. Pokvareni i krivotvoreni IoT uređaji

Značajan IoT sigurnosni izazov je zatvaranje perimetra i upravljanje svim uređajima jednog korisnika. Nagli porast popularnosti i obima proizvodnje uređaja Internet of Things dovodi do problema kućnih mreža.

Bez ikakvog odobrenja, korisnici instaliraju neispravne i krivotvorene IoT uređaje u zaštićene mreže. Te jedinice ili zamjenjuju izvorne ili se integriraju u mrežu za prikupljanje povjerljivih informacija i podataka, čime se ruši mrežni opseg.

Ti se uređaji mogu pretvoriti u netačne pristupne točke, video kamere, termostate i druge vrste uređaja za krađu komunikacijskih podataka bez korisnikova znanja.

6. Nedostatak korisničke svijesti o sigurnosti Interneta stvari

Budući da je Internet stvari tako nova tehnologija, korisnici se još uvijek navikavaju na njegove hirove i osobine.

Ljudi su u velikoj mjeri savladali vlastitu sigurnost u domenama krađe identiteta, napada virusa i zlonamjernog softvera na svojim računalima i internetskim prijevarama. Naučili su kako osigurati svoje WiFi mreže i kako zaštititi svoje kreditne kartice na mreži.

Ali, što se tiče sigurnosnih pitanja IoT-a, i njih se može pripisati nedostatku obrazovanja i zanemarivanju korisnika, koliko god oni ležali na proizvođačevim plećima.

Ovo neznanje korisnika i nedostatak svijesti vjerojatno su najveća briga za sigurnost Interneta stvari, jer može ugroziti sve: i same korisnike, kao i one koji su na ovaj ili onaj način povezani s vlastitim IoT jedinicama.

Napadi socijalnog inženjeringa iskorištavaju ovu jednostavnu činjenicu da je ljudski faktor najlakše zaobići ciljanjem ljudi koristeći Internet stvari.

Naročito težak primjer takve zlouporabe nepripremljenog ljudskog faktora bio je razorni napad na nuklearno postrojenje u Iranu 2010. godine. Cilj je bio IoT uređaj nazvan programabilni logički kontroler i trebao je samo jedan radnik da priključi USB bljeskalicu u jedno od internih računala kako bi poremetio izolaciju interne mreže od javne, što ju je učinilo ranjivom na napad.

Osnove IoT sigurnosti za preduzeća

Kompanije su veoma dobro svjesne potencijala IoT tehnologije. Zapravo, kompanije širom svijeta prihvaćaju IoT kao sredstvo za jasniju komunikaciju i procese. IoT uređaji mogu kompaniji pružiti veoma korisne uvide do kojih nije lako doći bilo kojom drugom tehnologijom.

Ipak, poduzeća se i dalje bore s osnovama IoT sigurnosti. Naravno, ovo stvara nove ranjivosti u cyber sigurnosti koje mogu značiti katastrofu. Zbog toga je normalno da se sve više postavlja pitanje kako kompanije mogu spriječiti vanjske prijetnje koje mogu prodrijeti u njihov digitalni ekosistem putem krajnjih tačaka na kojima su IoT uređaji?

Kako bi obezbjedili da vaš IoT projekat bude što bolje zaštičen od vanjskih prijetnji, važno je da razumijete izazove od kojih zavisi sigurnost vašeg projekta.

To su:

1. Zašto su osnove IoT sigurnosti bitne

Svaki razgovor o osnovama IoT sigurnosti mora sadržavati razloge zašto uređaji predstavljaju takvu prijetnju cyber sigurnosti.

Nažalost, dizajneri IoT uređaja rijetko uključuju opsežni sigurnosni firmware krajnje točke u svoje proizvode. U stvari, postojanje bilo kakve cyber sigurnosti na uređajima pokazuje rijetkost. To ih iz blagodati poslovnog procesa pretvara u ozbiljnu slabost.

Komplicirajući problem, čak i oni uređaji s zaštitom krajnje točke čine njegovo održavanje nezgodnim. Obično proizvođači javno ne najavljuju sigurnosne zakrpe, često prisiljavajući poduzeća da sustignu činjenice. Uz to, ažuriranje i krpanje IoT predmeta može stvoriti poteškoće; Tim IT sigurnosti mora za to potrošiti dragocjeno vrijeme i resurse.

Konačno, zaštita krajnje točke ugrađena u IoT uređaje rijetko se pokaže dovoljnom za suprotstavljanje suvremenim cyber prijetnjama.

2. Razumjevanje posljedica neuspjeha u obezbjeđenju osnova IoT sigurnosti

Sad kad razumijete rizike povezane s IoT-om, morate se pomiriti i s posljedicama tih rizika. Bez ovog znanja, vaši napori da ispravite ovaj sigurnosni problem krajnje točke mogli bi propasti; motivacija djeluje bolje s predznanjem potencijalnih rezultata.
Zapravo, poduzećima je ovo predznanje potrebno više nego ikad. Nedavno istraživanje tvrtke Trend Micro ukazuje na to da poduzeća ne razumiju posljedice neuspjeha u osnovama IoT sigurnosti:

Samo 50% IoT-ovih donositelja odluka u poduzećima prepoznaje IoT kao potencijalnu sigurnosnu ranjivost krajnje točke.

Još gore, 43% smatra da je IoT-ova sigurnost u njihovim strategijama implementacije promišljena.

52% poduzeća kaže da je gubitak povjerenja kupaca glavna posljedica kršenja IoT podataka.

49% kao najveću posljedicu navodi novčane gubitke.

63% ispitanika kaže da su se napadi IoT uređaja povećali posljednjih godina.

Međutim, neuspjeh u provođenju osnova IoT sigurnosti može rezultirati još gorim posljedicama. IoT uređaji mogu mjesecima prikrivati prijetnje skrivene viruse poput malware-a za rudarenje kriptovaluta. U drugim slučajevima IoT uređaji pružaju uporište hakerima za napade. U najekstremnijim scenarijima hakeri mogu čak koristiti IoT za gašenje mreža, što uzrokuje strašni zastoj.

3. Shvatite opseg vašeg rizika

Kako su istaknuti i rizici i posljedice neuspjeha u osnovama IoT sigurnosti, možemo početi istraživati korake za njihovo ublažavanje. Očito je da prvi korak za ublažavanje rizika jest razumijevanje vlastitog.

Kao što već znate broj IoT uređaja će značajno rasti u narednim godinama. Stoga vjerovatno je da će istovremeno rasti broj IoT-ovih sigurnosnih napada. I ti napadi će se širiti nego što ih većina poduzeća može prilagoditi i zaštititi.

Stoga je jedna od osnova IoT sigurnosti razumijevanje koji se uređaji redovito povezuju s vašom poslovnom infrastrukturom. Često se to pokaže puno lakše reći nego učiniti. IoT uređaji imaju notornu reputaciju jer nisu vidljivi na vašoj mreži tijekom sigurnosnih pregleda i istraga. U stvari, oni se možda uopće neće pojaviti na mreži.

Stoga ovo IoT uređaje čini glavnim "tamnim" područjem i za infiltraciju i za podmetanje skrivenih cyber napada. Da biste se borili protiv toga, trebali biste upotrijebiti IoT sigurnosno rješenje svog poduzeća za provođenje digitalne revizije svih uređaja. Osim toga, možete obaviti fizičku (ako je opsežna) reviziju lokalnih uređaja ili istraživanje udaljene radne snage. Srećom, većina sigurnosnih rješenja krajnjih točaka nude centralizirane nadzorne ploče upravo iz tog razloga.

4. Koristite IoT Cloud

Smještaj IoT projekta u Cloud sada je apsolutno neophodno, posebno za poduzeća s hibridnom ili informatičkom infrastrukturom koja se temelji na Cloud-u. Integriranje IoT stavki u Cloud omogućuje lakšu integraciju s mrežom prilikom dodavanja novih uređaja. To omogućuje vašoj sigurnosti u Cloud-u i hibridnoj sigurnosti krajnje točke da prepoznaju i zaštite IoT uređaje.

Štoviše, IoT integracija s Cloudom čini digitalnu transformaciju daleko lakšom i dugoročno sigurnijom.

5. Šifriranje, šifriranje, šifriranje

Većina IoT komunikacija i prometa ostaje nešifrirana.

Kao rezultat toga, hakeri mogu lako presretati, ometati, promatrati, kopirati i na drugi način manipulirati tim komunikacijama.

Vaša IoT sigurnost ovisi o šifriranju ovih komunikacija, baš kao što biste trebali i bilo koje druge vrste osjetljivih komunikacija. To se pokazuje osnovno što se tiče osnova, ali ne manje važno.

6. Slijedite najbolje primjere iz prakse za IoT

Osnove IoT sigurnosti ponekad se pokažu jednostavnim poput zdravog razuma. Ipak, bez znanja koje ga prati, ove najbolje IoT prakse također se ignoriraju.

Ove najbolje prakse uključuju:

- Isključivanje i odspajanje IoT uređaja dok se ne koriste. Ne dajte hakerima još jedan potencijalni vektor kibernetskog napada, osim ako to nije prijeko potrebno.
- Ograničavanje broja IoT uređaja koji se povezuju ili smiju povezati s vašom mrežom.
- Odabirom kupovine IoT uređaja za stavke koje možete ažurirati na daljinu.
- Osiguravanje da se svi IoT uređaji mogu integrirati s vašom trenutnom ili nadolazećom sigurnosnom platformom krajnje točke.

Primjena ovih praksi tijekom rada sa sveobuhvatnim sigurnosnim rješenjem krajnje točke može vam pomoći ojačati vašu IoT obranu.

7. Bez postavljanja i zaborava

Jedna od osnova moderne kibernetičnosti pokazuje se jednako istinitom i za IoT sigurnost: ne možete je "postaviti i zaboraviti".

Za mnoga poduzeća ovo načelo stvara kamen spoticanja. Uopšte se donositelji odluka sjećaju razdoblja kada ste jednostavno mogli kupiti antivirusno rješenje i ostaviti ga na tome. Ponekad njihove odluke odražavaju ta sjećanja.

Ali ti su dani prošli. IoT sigurnost ne može se "postaviti". Umjesto toga, vaše projekat se mora kontinuirano baviti evaluacijom i ispravljanjem tečaja kako se pojave nove prijetnje i kada se vaša infrastruktura razvija. Morate osigurati da optimalno implementirate i održavate svoju zaštitu krajnje točke kako biste osigurali IoT sigurnost, a to možda neće nalikovati prethodnim implementacijama.

Osnovna razmatranja sigurnosti IoT projekta

Kao što smo to pomenuli u prvom dijelu priručnika, vaša IoT sigurnosna razmatranja trebala bi sadržavati najmanje:

- Pristup krajnjoj točki
- Šifriranje podataka po potrebi

- Odgovarajuća autentifikacija

Upoznajmo se malo bolje sa svakim od ovih razmatranja.

Pristup krajnjoj tačci

Prema nedavnom izvješću F-Secure, uređaji Internet of Things (IoT) pretrpjeli su 760 milijuna napada u prvoj polovici 2019. Doista, sigurnosne prijetnje krajnjim točkama IoT uređaja porasle su za 300 posto u 2019. godini.

U nekom smislu IoT uređaji predstavljaju značajnu promjenu u IT infrastrukturi poduzeća; kao takve, mnoge sigurnosne prijetnje s kojima je suočene nalikuju prijetnjama drugih transformacijskih tehnologija. Uostalom, ništa se radikalno ne mijenja bez stvaranja nekih rizika, posebno tehnologija koja uključuje toliko mnogo uređaja. Takav je način s IoT uređajima za poduzeća.

Zbog toga je važno da razumijemo kako možemo smanjiti sigurnosne prijetnje IoT uređajima?

Promijenite zadane lozinke!

Znajte koje uređaje imate i gdje se nalaze!

Riješite se starih uređaja!

Ako se ne može zakrpati, istrgnite ga!

To su neke od mojih preporučenih najboljih praksi kada je riječ o poslovnim IoT uređajima - bilo da se nalaze u uredima poduzeća, na terenu (od farmi do kioska u trgovačkim centrima), na stranicama kupaca ili se čak skrivaju u potrošačima (mislite na medicinske uređaje).

Pametni fotokopirni strojevi ili ručni skeneri koje koristi osoblje za dostavu paketa izgledaju kao da su novi zbog naziva "Internet stvari". Međutim, povezani i ugrađeni uređaji koriste se u poslovne svrhe već desetljećima i dobivaju novu pozornost.

Pojava staničnih podatkovnih modema i sveprisutna. WiFi i Bluetooth olakšali su postavljanje IoT uređaja. Jeftini mikroprocesori, memorija, senzori, baterije i radio uređaji znače da je cijena u nekim slučajevima pala na, ispod jednog dolara. To olakšava gubljenje traga za takvim uređajima - i zaboravljate da sve što je povezano s našom korporativnom mrežom ili Internetom postoji i rizik od kršenja i potencijalna prijetnja ako se ugrozi, a zatim podmeće da našteti nama ili drugima , elektroničkim putem ili u stvarnom svijetu.

Evo pet prijedloga za poduzeća koja trenutačno koriste ugrađene ili IoT uređaje (što je vjerojatno većina njih) ili razmatraju (što je većina ostatka). Sve što je povezano na mrežu mikroprocesorom je IoT uređaj, bez obzira razmišljate li o tome tako ili ne. To znači rizike. Sigurnost nije opcija - ona je u potpunosti potrebna.

1. Potražite sigurnosne podatke kod proizvođača uređaja

Prije nego što bilo što priključite na svoju mrežu (ili dopustite daljinsko povezivanje), provjerite razumijete li njezine sigurnosne osnove. Koje su ugrađene sigurnosne značajke, poput ROM-a (memorija samo za čitanje) s kojih se pokreće? Koje su zaštite ugrađene u njegov operativni sustav i mikroprocesore? Odakle dolaze zakrpe i kako ih dobavljač isporučuje vama (ili uređaju)?

Još pitanja: Možete li daljinski upravljati uređajem ili ga po potrebi ubiti ili to dobavljač može učiniti ako vi ne možete? Ako postoji kršenje ili prijavljena ranjivost, koje će kanale dobavljač koristiti da vas obavijesti? Koliko brzo će prodavač obećati odgovoriti? Postoje li jamstva na razini usluge o brzini isporuke zakrpa? Puno i puno pitanja. Trebate odgovore. Ako vam se ne sviđaju odgovori, nemojte instalirati uređaj - jer čim to učinite, preuzeli ste sav rizik.

2. Upotrijebite robusnu autentifikaciju i šifriranje

Prva misao o provjeri autentičnosti je: Ako postoji administrativna prijava na uređaj, provjerite je li uređaj zaštićen korisničkim imenom i lozinkom - a niti jedna još uvijek nije tvornički zadana. Također se pobrinite da nitko ne može izvršiti fizički reset (spajalicom) i vratiti uređaj na zadane administrativne podatke za prijavu i lozinku. Isto vrijedi i za daljinsko upravljanje, bilo da je to ugrađeni web poslužitelj, tekstualna konzola ili SNMP.

To je samo početak. Podaci idu u oba smjera. Pazite da podatke koji prelaze s uređaja u vaš podatkovni centar ili u uslugu u oblaku mogu primiti samo ispravni primatelji. Također pripazite da se na IoT uređaj mogu slati samo podaci iz ovlaštenih izvora. Razmislite o upotrebi VPN-ova ako je moguće kako biste osigurali da je uređaj na sigurnoj mreži. To je osobito istinito ako, na primjer, imate posla s prijenosnim ili mobilnim uređajem koji je povezan putem WiFi-a. I šifriranje - dobro, vjerojatno svi razumiju zašto ništa ne bi trebalo ići putem jasnog teksta i zašto bi šifriranje trebalo biti jako, ažurno i ne koristiti buggy protokole ili knjižnice.

3. Osigurajte da se uređaji mogu nadograditi bežično

Nedavno su ažuriranja softvera ugrađenih uređaja zahtijevala fizički pristup uređaju, zamjenu ROM-a, priključivanje RS-232 patch kabela ili stavljanje uređaja u način "ažuriranja". U današnje vrijeme to zaboravite. Uređaje je potrebno ažurirati "bežično"

(koristimo tu frazu čak i ako je uređaj fizički povezan s mrežom), ili se uopće neće ažurirati.

Postoje pitanja. Tko pravi ažuriranja, vi ili dobavljač? Najbolje je ako možete, tako da možete testirati ažuriranja i zakazati guranje. (Ponekad ažuriranja mijenjaju sigurnosne postavke, što je jedan od razloga zašto trebate testirati.) Trebale bi biti odredbe koje osiguravaju da samo ovlašteni korisnici (ili ovlašteni poslužitelji) mogu ugurati novi softver u uređaje, bilo da se radi o firmwareu, operacijskim sustavima ili aplikacijama koje borave u sjećanju.

U slučaju povremeno povezanih uređaja, svakako utvrdite želite li da se ažuriraju čim se povežu ili je to nezgodno za korisnika. Provjerite jeste li zaduženi za ažuriranja i da li vaš sustav upravljanja imovinom zna što je ažurirano i gdje ažuriranja možda nisu uspjela. Događa se.

4. Odmah uklonite nesigurne i stare uređaje

Uređaji stare. Proizvođač može ukinuti ugovore o podršci i ispravke programskih pogrešaka. Ponekad postoji sigurnosna pogreška koja se zaustavlja i koja se jednostavno ne može otkloniti firmwareom. Obavezno znajte za te situacije - i ne ostavljajte te uređaje aktivnima duže nego što je potrebno. Ako možete brzo zamijeniti hardver, sjajno. Ako ne, razmislite o deaktiviranju uređaja ili barem zahtijevanju od korisnika da predaju opremu.

Sve ovo može biti vrlo nezgodno u IoT domeni - snimanje medicinskih uređaja, poljoprivreda, daljinska telemetrija i tako dalje. Puno je teže od planiranja zamjene prijenosnih računala svake tri ili pet godina! Dobivanje novih uređaja, a zatim zakazivanje i obavljanje zamjene uređaja može potrajati puno vremena i koštati puno novca. To je šteta, ali uzmite u obzir rizik od ostavljanja nesigurnih i nepodržanih uređaja na terenu ili na mreži.

Da naglasimo: trebate sposobnost brisanja i isključivanja uređaja ako su oštećeni, ukradeni, izgubljeni ili bilo što drugo. Uvjerite se da je to sposobnost vašeg sustava upravljanja imovinom i IoT uređaja koje kupujete i implementirate.

Šifriranje podataka po potrebi

Internet stvari (IoT) donosi novi niz sigurnosnih problema. Za razliku od VPN šifriranja, koje štiti mreže šifriranim i anonimnim tunelom, IoT uređaji moraju biti ugrađeni sa svojim vlastitim jakim standardima sigurnosti i šifriranja.

VPN dodjeljuje izolirani prostor na mreži. Međutim, unutar VPN prostora, svim sudionicima može pristupiti svim mrežnim čvorovima. Kad su IoT uređaji vani, VPN ima mnogo otvorenih vrata.

Jedan je londonski kasino naučio tu lekciju na teži način. Hakeri su mogli ući u bazu podataka kockara u kockarnici. Ušli su putem terminala za akvarij za ribu povezanog s internetom kasina. Uljezi su uspjeli pristupiti bazi podataka i povući je preko mreže gore u Cloud-u kroz nezaštićeni termostat. Dakle, osobni i financijski podaci londonskih casino high rollera pobjegli su u divljinu putem bezazlene kontrole spremnika za ribu.

A izazov raste. Očito je da IoT raste i nastavit će rasti u sljedećih nekoliko godina. U IoT-u se koriste uobičajene metode šifriranja. U SAD-u, za razliku od Europe, ne postoji jedinstveni nacionalni zakon koji regulira prikupljanje i upotrebu osobnih podataka. Umjesto toga, američke tvrtke regulirane su raznim saveznim i državnim zakonima - HIPAA i FINRA, na primjer - pokrivajući kršenja podataka i neovlašteno otkrivanje osobnih podataka.

Međutim, postoje IoT standardi šifriranja. Proizvođači znaju da šifriranje mora biti srebrni metak kako bi zaštitili svoje proizvode i potrošače. Što se tiče standarda za IoT, najčešće metode šifriranja su:

1. Standard za šifriranje podataka (eng. Data Encription Standard - DES).

Nacionalni institut za standarde i tehnologiju američke vlade (NIST) nadgleda ovu formalnu metodu šifriranja ili DES. DES koristi isti ključ za šifriranje za šifriranje i dešifriranje podataka. Pošiljatelj i primatelj moraju imati isti privatni ključ. Potonji postupak poznat je kao algoritam simetričnog ključa.

Važna razlika između DES i AES (opisana u nastavku) je ta što je DES manje siguran od AES. Zapravo je DES šifriranje rezultat 30 godina starog napora američke vlade da pruži kriptografsku sigurnost za sve vladine komunikacije. Cilj je bio postići i kriptografsku sigurnost i standardizaciju. DES je kamen temeljac kriptografije, ali od tada su istraživači provalili.

2. Američki vladin napredni standard šifriranja (eng. The U.S. Government Advanced Encryption Standard - AES)

AES koristi jedan ključ za šifriranje različitih duljina. AES algoritam koncentrira se na jedan blok podataka i ponovno ga šifrira 10 do 14 puta, ovisno o duljini ključa.

Kada koristi medicinski uređaj povezan s internetom, AES ispunjava zahtjeve američke vlade za zaštitu podataka HIPAA. AES također ispunjava FINRA standarde za zaštitu financijskih evidencija. AES je učinkovit i elegantan algoritam čija snaga leži u ključnim opcijama duljine. Što je duljina ključa duža, to je eksponencijalno teže razbiti šifriranje.

3. Standard trostrukog šifriranja podataka (eng. Triple Data Encryption Standard - DES)

Ovaj algoritam je vrsta računalne kriptografije gdje svaki blok podataka prima tri prolaza. Dodatna sigurnost dolazi od veće duljine ključa. Trostruki DES zamijenio je NIST koji je usvojio gore spomenuti AES. Trostruki DES sada se smatra zastarjelim, ali ga neki IoT proizvodi i dalje koriste zbog njegove kompatibilnosti i fleksibilnosti.

Ono što trostruki DES dobro radi je zaštita od napada grubom silom. Gruba sila iscrpni je napor (za razliku od intelektualnih strategija) ponovljenim pokušajima i naporima. Napadi grubom silom koriste automatizirane alate za pogađanje raznih kombinacija dok haker ne pukne ključ.

4. RSA enkripcija (eng. RSA Encryption)

Inicijali RSA potječu od prezimena trojice osnivača RSA Data Security (Rivest, Shamir i Adelman). RSA enkripcija koristi tehnologiju šifriranja s javnim ključem licencu RSA Data Security, koja također prodaje pripadajuće razvojne setove.

RSA enkripcija omogućuje korisnicima slanje šifriranih podataka bez prethodnog dijeljenja koda s primateljem. To je šifriranje javnog ključa i javni se ključ može otvoreno dijeliti. Međutim, podatke može dešifrirati samo drugi privatni ključ. Svaki korisnik RSA ima zajednički javni ključ, ali privatni ključ imaju samo određeni primatelji.

5. Twofish enkripcijski algoritam

Twofish je još jedan algoritam blok šifre koji je Counterpane Labs predložio prije više od 20 godina kao zamjenu za AES. Twofish je bio finalist za izbor kao novi NIST Advanced Encryption Standard, ali nije odabran.

Twofish koristi sustav blok šifriranja koji se temelji na jednom ključu bilo koje duljine do 256 bita. Ovaj standard šifriranja učinkovit je na računalima s procesorima manjeg kapaciteta i pametnim karticama IoT uređaja. Twofish se pojavljuje u mnogim besplatnim softverskim proizvodima za šifriranje, poput VeraCrypt.

Odgovarajuća autentifikacija

Pod odgovarajućom auntentifikacijom podrazumjevamo da vaš IoT projekat ima ugrađenu provjeru autentičnosti.

Što je IOT provjera autentičnosti?

Sposobnost zaštite podataka i ograničavanja na one koji imaju točna dopuštenja nije nova ideja i često se koristi u mnogim industrijama. Može se samo zapitati zašto povezani uređaji od početka nisu podlijegali istim sigurnosnim načelima.

Jednostavno je previše kategorija IoT uređaja da bi se spomenuli u postu ove veličine, ali oni se uvelike razlikuju u pogledu razine sigurnosti. Neki se povezuju pomoću bliskih protokola kao što su Bluetooth, RFID (identifikacija radio frekvencije) ili Wi-Fi, dok drugi koriste GPS, 4G ili su ožičeni. Povezati ih često je lako poput traženja uređaja u blizini, unosom kratkog koda (koji se može ili ne mora mijenjati prema zadanom) ili upotrebom oblika višefaktorske provjere autentičnosti za provjeru dozvola uređaja i primatelja.

Primjeri IoT-a različiti su poput IoT-ovih proizvoda koje koriste, ali trenutni trendovi sugeriraju da dolazi do promjena, iako će trebati neko vrijeme da se filtrira do svih proizvođača uređaja. Većini nas je poznata internetska kupovina. Biste li kupili u trgovini koja ne koristi SSL, gdje se simbol zaključavanja prikazuje u nekim preglednicima ili adresa počinje s https? Sličan pristup IoT uređajima je vjerojatan i poznat je pod nazivom PKI (infrastruktura javnog ključa) gdje digitalni certifikati dokazuju autentičnost web mjesta ili u ovom slučaju IoT uređaja.

Digitalni certifikati osigurali bi razinu povjerenja u IoT uređaj koji inače nedostaje i, u kombinaciji s IoT aplikacijama za nadgledanje infrastrukture, mogli bi identificirati i spriječiti pristup neovjerenim uređajima sa slabom sigurnošću.

Vi možete primeniti nekoliko IoT metoda provjere autentičnosti.

Bez obzira na način provjere autentičnosti, cilj je IoT sigurnosti. Možete zaključiti da je dvofaktorska provjera autentičnosti dovoljna ili da vam bude potreban SSO (jedinstvena prijava) radi praktičnosti. Možda ćete htjeti koristiti Azure IoT za upravljanje svim uređajima. Možda imate posebne zahtjeve za kvalitetu usluge koji zahtijevaju upotrebu MQTT klijenta. MQTT (Telemetry Transport u redovima poruka) protokol je za razmjenu poruka i jedan od mnogih koji IoT uređaji možda koriste.

Međutim, IoT uređaji koriste široku paletu protokola i standarda, a vaše metode provjere autentičnosti moraju uzeti u obzir ovu varijaciju. Stoga je poznavanje ovih varijacija nužno, a potrebno je blisko poznavanje kupljenih IoT uređaja kako bi se osiguralo da svaki uređaj može provjeriti autentičnost na siguran način. Nekima će možda trebati ručno ažuriranje (nedostaje OTA funkcionalnost), a drugima su zaključane

postavke koje se ne mogu promijeniti prema zadanim postavkama. Možda će IoT platforma automatizirati većinu vaših zahtjeva?

Zaključno, IoT metode provjere autentičnosti potrebne su za osiguranje IoT uređaja i postoji nekoliko načina za postizanje ovog cilja. Neki mogu dodijeliti namjenske IoT mreže, žrtvujući korisne značajke u ime sigurnosti. Imajte na umu da je moguće sve integrirati na način koji je i siguran, ali morate osigurati da su uređaji dizajnirani sa sigurnošću. Kao rezultat toga, možda ćete trebati isključiti neke uređaje, ali to je sigurno mala cijena za mir i sigurnu infrastrukturu?

2. Otklanjanje IoT cyber prijetnji

Dizajniranje sigurnih IoT aplikacija;

Novo doba IoT povezivanja, prikupljanja podataka i upravljanja objektima fizičkog svijeta uvodi nove sigurnosne rizike, od sofisticiranih automatiziranih cyber napada do hakera koji su vraški u krađi podataka i izazivanju pustoši. Sigurnost IoT uređaja u velikoj je mjeri ovisna o softveru i aplikacijama koji se koriste za upravljanje njima, što programere postavlja na cyber front-line liniju i što zahtijeva da znaju kako razviti sigurne IoT aplikacije.

U ovoj sekciji iznijećemo najbolje prakse za tehnike sigurnog kodiranja i sigurnosne funkcije koje će razvojnim timovima pomoći u stvaranju elastičnih IoT aplikacija koje ublažavaju sigurnosne rizike IoT-a.

Dizajniranje sigurnih IoT aplikacija

U fazi planiranja ili dizajniranja IoT aplikacije mora postojati formalna procjena zahtjeva za sigurnost i privatnost planirane aplikacije od vrha do dna.

Razvoj IoT aplikacija zahtijeva pristup "Sigurnost dizajnom". Ovaj pristup znači razmatranje sigurnosnih zahtjeva svih IoT-ovih aplikacijskih funkcija kao dio faze dizajniranja, umjesto pretpostavke i primjene sigurnosnih značajki kasnije u procesu razvoja. Kao i svaka druga greška ili problem, skuplji je i treba više vremena da se ispravljaju sigurnosni problemi u kasnijim fazama razvoja.

Stoga je u fazi dizajniranja aplikacije neophodno razmotriti i planirati sve moguće sigurnosne zahtjeve za IoT aplikaciju.

Pregled sigurnosnih zahtjeva

U fazi projektiranja pregledajte sigurnosne zahtjeve za svoju IoT aplikaciju dovršavanjem pregleda slijedećih sigurnosnih zahtjeva:

- Planirajte funkcije upravljanja korisničkim računom. Osigurajte da IoT aplikacija ima odgovarajuću razinu prilagodbe računa.
- Dizajnirajte siguran mehanizam za poništavanje lozinke. Ovaj se postupak često zanemaruje u korist korisničke udobnosti, ali slab postupak poništavanja lozinke može pružiti lako zaostajanje u sustavu.
- Dizajnirajte strukturu korisničkog računa kako biste ograničili privilegije administrativnog računa na osnovi potrebe. Pametno je odvojiti administrativne radnje i prava od standardnih korisničkih računa jer ova konfiguracija ograničava rizik od pogrešne konfiguracije od strane korisnika, što može dovesti do ozbiljnih sigurnosnih rupa.
- Utvrdite kako će aplikacija spremati lozinke računa. Mora se izbjegavati pohrana lozinki u običnom tekstu u baze podataka i ravne datoteke. Najbolja praksa je koristiti algoritam slanog raspršivanja, poput SHA-256 i soli, za izračunavanje lozinki u jedinstvenu vrijednost raspršivanja, što znači da se lozinke ne mogu vratiti natrag u običan tekst.
- Razmislite o dodavanju funkcije dvofaktorske provjere autentičnosti, posebno za aplikacije koje će obrađivati povjerljive podatke kojima je namijenjen pristup iz nepouzdanih mreža.
- Razmislite o dodavanju podrške za integraciju IoT aplikacije sa sustavima za upravljanje računima, poput Microsoft Active Directory Services. Ova sposobnost pomaže integrirati IoT aplikacije u poslovna poslovna okruženja.
- Ako osobne ili povjerljive podatke planirate pohraniti u okruženja trećih strana ili u nepouzdana okruženja, razmislite o upotrebi šifriranja za zaštitu podataka u mirovanju.
- Dizajnirajte mogućnost ažuriranja softvera koja osigurava primjenu samo digitalno potpisanih (izvornih) ažuriranja, a ako je izvedivo, razmotrite postupak automatskog ažuriranja.
- Osigurajte funkciju sigurnosne obavijesti koja omogućava aplikaciji da šalje sigurnosna upozorenja, poput neuspjelih pokušaja prijave, s poslovnim sustavom za nadzor sigurnosti ili syslog poslužiteljem.

- Pozovite sigurnosnog stručnjaka da izvrši reviziju i odobri sigurnosne funkcije i dizajn aplikacije.

Procjena utjecaja na privatnost

Tamo gdje IoT aplikacije prikupljaju, pohranjuju i obrađuju lične podatke, to moraju činiti u skladu s važećim zakonima o zaštiti podataka i privatnosti. Zakoni o privatnosti podataka mogu imati različite stupnjeve strogih zahtjeva, ovisno o tome kojoj zemlji pripadaju podaci građana. Procjena utjecaja na privatnost potrebna je kako bi se osiguralo da se aplikacija i IoT uređaj pridržavaju važećih zakona, uključujući pohranu ili obradu osobnih podataka u oblaku i treće strane.

Za procjenu uticaja na privatnost potrebno je da uradite slijedeće:

- Dokumentirajte i opravdajte svu planiranu upotrebu osobnih podataka od strane aplikacije.
- Prikupljanje osobnih podataka ograničite samo na ono što je prijeko potrebno.
- Razmislite o korištenju rutina za anonimiziranje osobnih podataka; postupak koji, kada se pravilno izvede, može ukloniti teret ispunjavanja zahtjeva za zaštitu privatnosti pravnih podataka.
- Planirajte napisati rutine ili upotrijebiti rješenja (poput SSL-a) koja šifriraju sve pohranjene osobne podatke i također dok se podaci prenose mrežama, uključujući privatne mreže.
- Osigurajte postojanje transparentnosti privatnosti kod potrošača. Svako prikupljanje, obrada i pohrana osobnih podataka, uključujući pohranu u oblaku, potrošaču mora biti jasno naznačeno u izjavi o privatnosti. Prije nego što upotrijebite osobne podatke, pribavite izričit pristanak korisnika i osigurajte da korisnik potpiše ili pristane na ugovor o privatnosti koji objašnjava svu upotrebu osobnih podataka u aplikaciji.
- Razmotrite druge vrste podataka koje podliježu industrijskim propisima. Osigurajte da su svi regulatorni zahtjevi u potpunosti razumljivi i da će ih se poštivati kao dio dizajna aplikacije.
- Razmotrite privatnost mobilne aplikacije. Mobilna aplikacija može se povezati s GPS-om, SIM karticama, identifikacijskim brojevima uređaja, podacima uređaja i podacima iz mobilnih aplikacija trećih strana. Sve ove interakcije mogu imati implikacije na privatnost na aplikaciju i moraju se uzeti u obzir.

Kodiranje sigurnih IoT aplikacija

Mnogo različitih vrsta aplikacija može kontrolirati i upravljati IoT uređajima, poput aplikacija u oblaku i lokalnih web aplikacija, mobilnih aplikacija i softvera koji se izvodi na samom IoT uređaju. Projekt sigurnosti otvorenih web aplikacija (OWASP) organizacija je koja se fokusira na to kako poboljšati sigurnost softvera. Ova organizacija ima projekt Internet of Things, koji okuplja jedinstvene aspekte IoT sigurnosti. Trenutno izrađuju IoT sigurnosne smjernice za proizvođače, programere i potrošače.

IoT web aplikacije: savjeti za sigurno kodiranje

Web aplikacije se obično koriste za upravljanje IoT uređajima. Bez obzira je li web aplikacija namijenjena hostiranju izravno s IoT uređaja, s internog mrežnog poslužitelja ili u oblaku, razvoj (kodiranje) tih web aplikacija mora biti u skladu s najboljim praksama razvoja sigurnosti web aplikacija, poput "**OWASP Top Ten**".

Uobičajena pogreška u razvoju IoT web aplikacija je što se marljivo ne osiguravaju web aplikacije privatne mreže u istoj mjeri kao i web aplikacije javne orijentacije. Međutim, interne mreže mogu biti ugrožene i postati nepouzdano okruženje. Stoga hakeri i zlonamjerni programi mogu iskoristiti ranjivosti web aplikacija okrenute prema unutrašnjosti.

Razmotrite ove savjete za sigurno kodiranje za IoT web aplikacije:

- Sanitizirajte sve korisničke unose.

  Ova tehnika kodiranja može spriječiti najčešće napade web aplikacija koji iskorištavaju loše kodiranu provjeru unosa korisničkih podataka za ubrizgavanje zlonamjernih skripti, pokretanje SQL naredbi baze podataka i izvođenje prekoračenja međuspremnika. Stoga je osnovna praksa kodiranja aplikacija da se sva korisnička polja za unos očiste kako bi prihvatila samo "bijeli popis" očekivanih znakova. Svakako, kodirajte provjeru na strani klijenta unutar web preglednika (kao što su Java skripte), ali sanacija unosa uvijek se mora dogoditi unutar (poslužiteljske) aplikacije jer se većina hakova pokušava ubrizgavanjem koda kroz URL.

- Sigurno koristite kolačiće.

  Kada aplikacija koristi SSL kako bi osigurala da aplikacija označava kolačiće kao sigurne, SSL ih automatski automatski šifrira. Kada web aplikacija nije namijenjena SSL zaštiti, kodirajte rutinu za šifriranje vrijednosti kolačića industrijskim algoritmom šifriranja, poput AES 256.

- Zaključajte izvještavanje o pogrešci aplikacije.

  Poruke o pogreškama aplikacije mogu hakerima pružiti naznake o tome kako provaliti u aplikaciju i korisničke račune. Čak i najjednostavnija poruka pogreške, poput "netočne korisničke lozinke", može otkriti da je ime korisničkog računa točno pretpostavljeno.

- Koristite rutine za šifriranje podataka.

  Ako vam je aplikacija potrebna za šifriranje osobnih ili povjerljivih podataka, ne pokušavajte pisati vlastite rutine šifriranja. Umjesto toga, koristite knjižnice koje koriste metodologije i algoritme šifriranja priznate u industriji.

- Provjeravjte sigurnosne usluge trećih strana.

- Procijenite i dokumentirajte sigurnost knjižnica trećih strana koje aplikacija koristi prije nego što ih upotrijebite, a zatim ih neprestano nadgledajte zbog sigurnosnih ranjivosti i zakrpa. Na primjer, nedavno je utvrđeno da OpenSSL, biblioteka otvorenog koda koja se koristi za šifriranje podatkovne komunikacije, ima kritične nedostatke, čineći web aplikacije ranjivima na napad. Problem je brzo riješen izdavanjem ažurirane verzije knjižnice.

- Provjerite jesu li svi programeri, uključujući dobavljače i treće strane, kvalificirani i obučeni za upotrebu tehnika sigurnog kodiranja web aplikacija.

IoT aplikacije za mobilne uređaje: sigurni savjeti za kodiranje

Mobilne IoT aplikacije, posebno aplikacije za pametne telefone i tablete, aktivno su ciljane od strane hakera. Iste tehnike sigurnog kodiranja koje se koriste s web aplikacijama također su potrebne kada razvijate mobilne IoT aplikacije. Međutim, postoje dodatna razmatranja sigurnosti aplikacija, kao što su provjera autentičnosti mobilnih uređaja, telekomunikacije i SMS podatkovne komunikacije, te daljnji rizici privatnosti.

Razmotrite ove savjete za sigurno kodiranje za IoT aplikacije za mobilne uređaje:

- Procijenite integraciju aplikacije sa značajkama i mogućnostima vaše mobilne platforme i operativnog sustava, koje se mogu razlikovati ovisno o vrsti mobilne platforme i operativnom sustavu. Integriranje s mobilnim funkcijama može poboljšati sigurnost, ali također može oslabiti sigurnost aplikacije. Na primjer, upotreba biometrijskog skenera otiska prsta na Apple uređajima može poboljšati postupak provjere autentičnosti mobilne aplikacije; međutim, oslanjanje isključivo

na sustav provjere autentičnosti mobilnog uređaja koji se može onemogućiti, može ozbiljno oslabiti aplikaciju.

- Pazite da vaša IoT mobilna aplikacija štiti sve osobne i osjetljive podatke tijekom prijenosa te da se podaci šifriranjem pohranjuju na mobilni uređaj. Aplikacija mora prisiliti na upotrebu šifriranih mrežnih usluga putem Interneta i wifi veza (to jest, pretpostaviti da su javne), pa čak i podatke koji se šalju putem mobilnih mreža. Također, pobrinite se da aplikacija šifrira sve osobne podatke koji su pohranjeni na prijenosnim medijima.

Softver IoT uređaja: sigurni savjeti za kodiranje

Pored već obrađenih tehnika sigurne aplikacije, imate nekoliko dodatnih razmatranja u razvoju softvera koji će raditi na IoT uređajima, poput upotrebe firmvera i kontrole pristupa fizičkim sučeljima.

Razmotrite ove savjete za sigurno kodiranje softvera IoT uređaja:

- Obavezno koristite najnoviju verziju firmvera IoT uređaja.
- Pratite proizvođače firmvera za obavijesti o ažuriranjima firmvera i otkrivanje sigurnosnih ranjivosti firmvera.
- Testirajte nova izdanja firmvera s aplikacijom. Nova izdanja firmvera mogu zahtijevati ažuriranje aplikacijskog koda.
- Pregledajte zahtjeve za fizičkim sučeljima za vaš IoT uređaj, od kojih aplikacija može zahtijevati funkciju kontrole pristupa.
- IoT aplikacije moraju se moći ažurirati sigurnosnim zakrpama. Zakrpe moraju biti digitalno potpisane i potvrđene postupkom ažuriranja aplikacije prije instalacije kako bi se osiguralo da se zlonamjerne zakrpe ne mogu instalirati.
- IoT aplikacije trebaju šifrirati sve osobne podatke, kao i osjetljive IoT uređaje i podatke aplikacija, koji su namijenjeni pohrani na prijenosni medij IoT uređaja (odnosno memorijske kartice).

Testiranje sigurnosti u IoT aplikacijama

Jedna od najučinkovitijih tehnika u prepoznavanju sigurnosnih nedostataka i slabosti u fazi razvoja, bez obzira na vrstu IoT aplikacije, je dovršavanje pregleda koda. Preglede koda trebaju provoditi odgovarajuće kvalificirani programeri kodera koji su idealno neovisni o razvojnom projektu. Osigurajte da je pregled koda formalno temeljit postupak i razmislite o korištenju programera koji rade na različitim projektima i upotrebi alata kao što je IBM Security AppScan Source. AppScan Source može rano unutar SDLC-a skenirati i identificirati ranjivosti izvornog koda weba i mobilnih aplikacija (prije faze testiranja). Podržava kôd napisan na JavaScript, HTML5, Cordova, Java, Objective-C ili poslovnoj mobilnoj platformi IBM Mobile Foundation.

Pregledi koda mogu se činiti skupim i dugotrajnim dodatkom SDLC-u, ali mogu donijeti velike dividende izbjegavajući skupa ponovna testiranja, izbjegavajući sigurnosne zakrpe nakon izdavanja i izbjegavajući štetu na vašem ugledu ako se ugrozi nesigurna IoT aplikacija. Pored pregleda koda u razvojnoj fazi, testna faza SDLC-a mora uključivati intenzivno sigurnosno testiranje, koje mora biti specifično za svaku vrstu IoT aplikacije.

Savjeti za sigurnosno testiranje internetskih aplikacija IoT

Izvođenje skeniranja ranjivosti i testova penetracije radi otkrivanja sigurnosnih nedostataka softvera ključni je završni korak prije puštanja IoT aplikacija. Testiranje aplikacijskog koda sprječava uobičajene ranjivosti aplikacija kao što su ubrizgavanje SQL-a, skriptiranje na više lokacija, krivotvorenje zahtjeva na više mjesta i napadi prelijevanja međuspremnika.

Razmotrite ove savjete za sigurnosno testiranje za internetske aplikacije IoT:

- Upotrijebite alat za skeniranje ranjivosti aplikacija kao što je IBM Security AppScan za sigurnosno testiranje aplikacije i prepoznavanje ranjivosti web aplikacija. Pogledajte vodič za developerWorks, „Skenirajte svoju aplikaciju da biste pronašli i riješili ranjivosti OWASP Top 10 2013“, za više informacija o ovom pristupu.
- Osigurajte da programeri razumiju probleme kada se otkrije nesigurno kodiranje aplikacija.
- Ne zaboravite osigurati sve API-je za testiranje.
- Izvršite test penetracije koji ponavlja pristup koji koriste vješti hakeri. Ispitivanje penetracije moraju provesti certificirani i iskusni etički hakeri (CEH). Pristup se smatra najboljom sigurnosnom praksom za bilo koju aplikaciju usmjerenu na Internet. Kompletna ispitivanja penetracije prije puštanja aplikacije, nakon bilo koje značajne promjene kodiranja, te na godišnjoj osnovi nakon toga.

- Osigurajte da ispitivači penetracije programerima mogu adekvatno objasniti pronađene ranjivosti i način njihove eksploatacije.

Savjeti za sigurnosno testiranje za IoT mobilne aplikacije

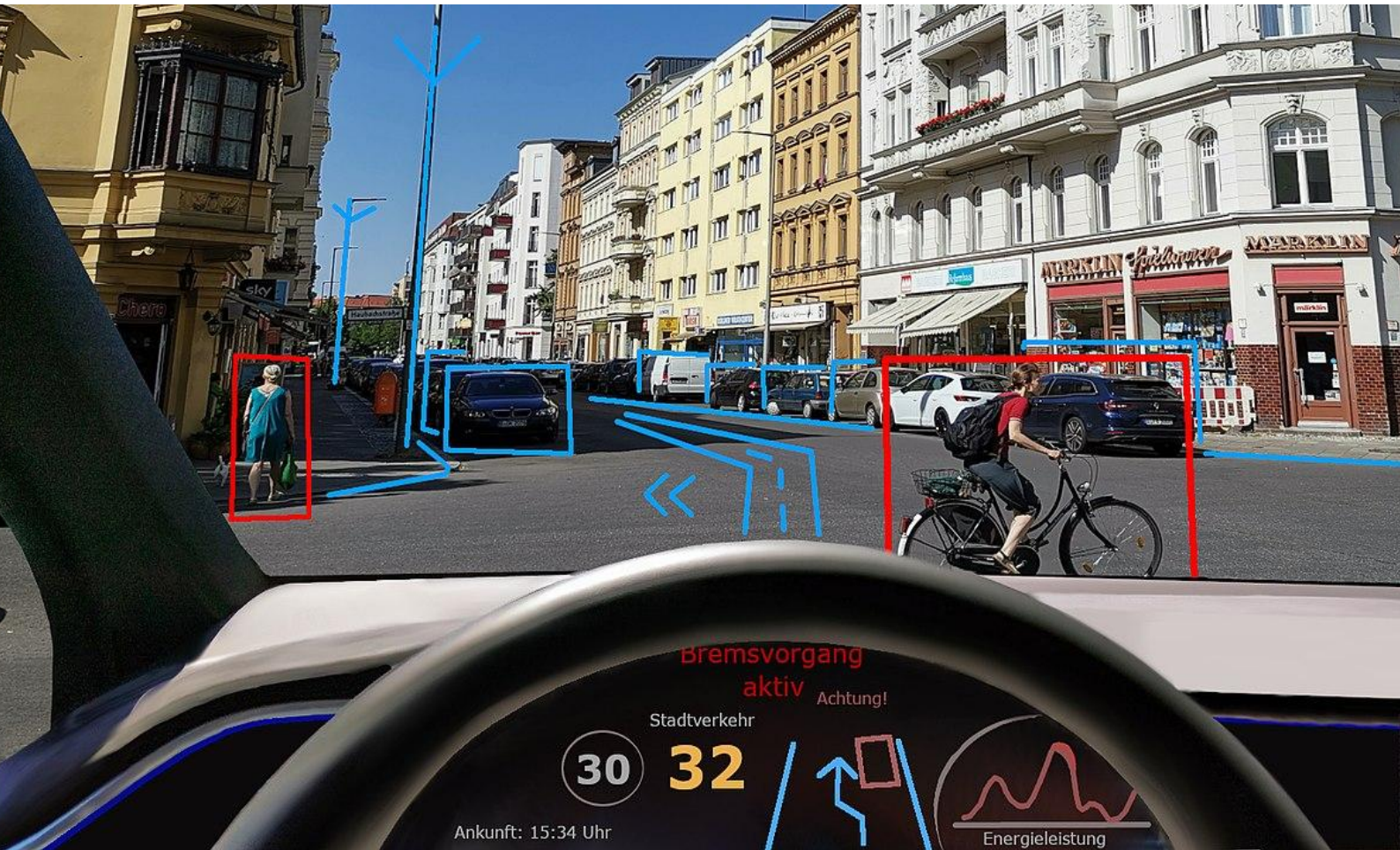
Koristite specijalizirani alat za skeniranje ranjivosti mobilnih aplikacija, kao što je IBM Application Security on Cloud, koji je posebno dizajniran za sigurnosno testiranje mobilnih aplikacija. IBM Application Security ne otkriva samo ranjivosti aplikacija za mobilne uređaje, već detaljno prikazuje ranjivost programerima, zajedno s razinom rizika i rješenjima za rješavanje ranjivosti.

Savjeti za sigurnosno testiranje softvera IoT uređaja

Softver IoT uređaja mora biti podvrgnut testiranju sigurnosnih stručnjaka i tvrtki specijaliziranih za pronalaženje ranjivosti softvera IoT uređaja.

Podaci i AI

Povezivanje svih stvari u Internet of Things



AITI

Skill Accelerator

Follow us at @UAITLab

Podaci i AI

Povezivanje svih stvari u Internet of Things

Početkom 20 stoljeća nafta je bila glavni motor do tada neviđenog progresa i napredka širom svijeta. Sto godina kasnije nafti se bliži kraj (kako zbog ograničenih resursa tako i zvog negativnog uticaja na okoliš) mjesto ključnog resursa na kojem se zasniva razvoj sve više preuzimaju podaci koji su glavni motor četvrte industrijske revolucija (Industrija 4.0).

U predhodnom poglavlju imali ste prilike kako bi napravili dobru strategiju. I kao što ste mogli primjetiti, korištenje ovih alata skoro pa bezvrijedno bez odgovarajućih, tačnih i relevantnih podataka.

Kako bi bili u mogućnosti da skoristite puni potencijal podataka u ovom poglavlju su obrađene teme koje će vam pomoći da usvojite znanja iz oblasti poslovnog obavještanja (Business Intelligence) čija primjena doprinosi boljem, bržem i efikasnijem donošenju odluka, te će steći vještine rada sa podacima u softverskim platformama za provođenje analitike podataka u poslovne svrhe.

U ovom poglavlju vi će te se moći upoznati sa:

- Osnovama pristupa poslovnog obavlještavanja i novim pristupima korištenja poslovnih podataka u procesu donošenja odluka u organizaciji;
- Osnovama rada sa podacima kako bi mogli iskoristiti njihov puni potencijal za primjenu poslovne analike u upravljačkim procesima;
- Mogućnostima koje nude softverkse platfome Tableau i Power BI, dvije trenutno najbolje softverske platforme za poslovnu analitiku i Business intelligence za mala i srednja preduzeća/organizacije.

Znanje sa kom se možete upoznati u ovom poglavlju sigurno će vam olakšati napore na razvoju vaših strateških ideja. Međutim, oni vam takođe mogu biti od izuzetne koristi kada budete razvijali vaše prijedloge projekata putem vi vaše strateške ideje razrađujete u detaljne planove akcije.

Poslovna analitika u doba podataka postaje sve važniji alat koji se primjenjuje u poslovanju, zato ne gubimo vrijeme i krenimo da se upoznamo sa ovom jako zanimljivom temom.

1. Inteligentni IoT

Prospekt inteligentnih IoT uređaja;

Prospekt inteligentnih ioT aplikacija

S valom ulaganja, nizom novih proizvoda i rastuće plima poduzetništva

raspoređivanja, umjetna inteligencija je praskanje u Internetu stvari (IoT).

Tvrtke koje izrađuju IoT strategiju, procjenjujući a potencijalni novi IoT projekt ili tražite više vrijednost iz postojeće IoT implementacije možda želi istražiti ulogu za AI.

Kakav je prospect inteligentnih IoT aplikacija dobro opisuju slijedeći podaci:

- Financiranje rizičnog kapitala za pokretanje IoT-a usmjerenih na AI brzo raste: u prvih osam mjeseci 2017. Godine ova je skupina start-upova prikupila 705 miliona USD
- Sve više se bilježi rast akvizicija IoT startupa koji su bazirani na AI;
- Dobavljači IoT platformi - uključujući Amazon, GE, IBM, Microsoft, Oracle, PTC, I Salesforce integriraju sposobnosti AI sa IoT
- Velike organizacije u različitim industrijama već koriste ili istražuju moć AI s IoT-om za pružanje novih ponuda i efikasniji rad,
- Gartner predviđa da će do 2022. više od 80% IoT projekata kompanija uključivati AI komponenta, od svega 10% u 2018. godini.

AI ključ za otključavanje IoT potencijala

Umjetna inteligencija igra sve veću ulogu u IoT aplikacijama, I ova promjena je očita u ponašanju kompanija koje posluju u tim područjima. IoT startupi koji u IoT koriste ai naglo se povećavaju.

Najveći pružaoci IoT softverskih platform sada nude integrisane AI mogućnosti kao što su Machine learning bazirane analize.

AI počinje da igra vodeću ulogu u IoT zbog njegove sposobnosti brzog izvlaćenja uvida iz podataka. *Machine learning* kao AI tehnologija donosi sposobnost automatskog identifikovanja orazaca I detektovanja anomalija u podacima koje prikupljaju IoT senzori – informacije kao što su temperature, pritisak, vlažnost, kvaliteta zzraka, vibracije i zvuk.

Kompanije otkrivaju da pomoću Machine learning mogu mati značajne prednosti u odnosu na tradicionalno poslovanje obavještajni alati za analizu IoT podataka, uključujući mogućnost izrade operativnih predviđanja do 20 puta ranije i s većom tačnosti od old-based sistema za monitoring.

I druge AI tehnologije kao što su prepoznavanje govora i *computer vision* mogu pomoći u izvlačenju uvida iz korištenih podataka koji obično zahtjevaaju da ih pregledaju ljudi kako bi se izvukli korisni uvidi.

Implikacije za preduzeća

Za preduzeća u različitim industrijama AI ima potencijal da podstakne vrijednost koju kreira IoT, omogućavajući pružanje bolje ponude i boljih operacija koje mogu dati konkurentsku prednost kroz veće poslovni performanse.

Rukovodioci u kompanijama trebali bi biti svjesni da sposobnosti predviđanja koje donosi Machine learning su sada integrisane u glavnim industrijskim IoT platformama, kao što su Microsoft Azure, IBM Watson IoT i Amazon AWS IoT.

U proizvodnji proizvoda široke potrošnje I trgovini, pojavljuje se sve više IoT rješenja koje koriste AI kako bi se predvidjela potražnja I optimizirao nivo zaliha.

Može se desiti vrlo brzo da bude jako teško pronaći IoT implementaciju koja ne koristi neku od prednosti koje donosi AI. Predviđanja govore da će u narednim godinama AI podržavati većinu efektvnih IIoT projekta I da će IIoT projekti koji budu bez AI pružati ograničenu vrijednost za kompanije.

Zbog toga, kada planirate iot bazirano rješenje, dobro razmislite kako u vašem planu da integrišete AI.

Kako upravljanje podacima koje generiše IoT

Posljednje poglavlje ovog priručnika fokusirano je na podatke i AI kako bi vam pomogli da dobijete maksimalnu korist iz vašeg IoT projekta.

U predhodnoj sekciji smo pokušali da vas ukratko upoznamo zbog čega je važno da vaš IoT projektat bude inteligentan I kakvu ulogu u tome ima AI.

AI svoju najveću snagu crpi iz podataka sa kojima raspolaže, a ioT senzori imaju potencijal da budu najveći generator digitalnih podataka.

Ali da bi vaši Machine learning algoritmi bili u mogućnosti da iz podataka izvlače podatke, vi morate veoma pažljivo da definišete kako će te upravljati podacima koje vaš IoT projekat generiše.

Vaši podaci žive na načine koji mogu značajno utjecati na vaše poslovanje. A budući da podaci u osnovi vode život samostalno, postoje pitanja koja trebate riješiti od samog početka vašeg IoT putovanja. Pitanja poput:

- Koliko ćete podataka prikupiti putem IoT uređaja?
- Koliko podataka šaljete i prenosite u Cloud?
- Što ćete učiniti sa svojim podacima?
- Koliko dugo ćete zadržavati podatkei?
- Trebate li arhivirati podatke kada vam više ne budu potrebni?

U ovoj sekciji nastojaćemo pojasniti zašto je upravljanje podacima ključno za održivu IoT strategiju i kako možete poduzeti prve korake u upravljanju valom podataka.

Zašto upravljati svojim podacima?

Kompanije često eksperimentiraju sa svojom IoT strategijom prije nego što pokrenu sveobuhvatne napore. Dokaz koncepta (eng. Proof of concept - POC) je jeftin pristup s malim rizikom koji vam može pomoći da pročistite strategiju.

Međutim, mnoga preduzeća koja su provela uspješnu IoT POC ili pilot studiju iznenađena su prelaskom na proizvodni model.

Poteškoće se javljaju projekt se povećava. Streamingom podataka s nekoliko povezanih uređaja može se upravljati, pohrana može postati problem kako se više uređaja povezuje s mrežom.

Nije moguće jednostavno se neograničeno držati svih podataka koje generiraju vaši povezani uređaji. Kao prvo, troškovi skladištenja uveoma lako mogu izmaći kontroli.

S druge strane, nema smisla hvatati podatke samo radi njihovog posjedovanja.

Umjesto toga, vaši vam podaci trebaju pomoći da postignete nešto određeno. Na primjer, riješite problem, poboljšajte operativnu efikasnost, pojednostavnite održavanje opreme ili smanjite otpad.

Ako stvarno želite da vaši podaci rade za vas - kako bi vam pomogli prepoznati obrasce, trendove i područja za poboljšanje - morate razumjeti kako tim podacima upravljati.

I zapamtite: Budući da nije moguće zadržati sve svoje podatke, potrebna vam je strategija upravljanja informacijama.

Zamislite što možete učiniti s podacima

Zamislite, na primjer, da želite razumjeti kako rasvjeta zgrade troši energiju. Instrumentacija vaše zgrade dobar je prvi korak. Ali povezana zgrada u stvarnom vremenu prikuplja podatke o mnoštvu faktora - od atmosferskog pritiska okoline, vlažnosti zraka, vremsnskih prilika do vanjske i unutrašnje temperature. Većina tih informacija nije presudna za razumijevanje utjecaja osvjetljenja na vaše račune za energiju.

Međutim, ono što bi bilo korisno znati jest jesu li svjetla stalno upaljena u praznim sobama ili ne. Ili bi li ih mogli smanjiti osvjetljenje po vedrom danu. Upravljanje podacima postupak je uzimanja ukupnih dostupnih podataka i njihovog pročišćavanja do nekoliko specifičnih mjernih podataka. IoT platforma trebala bi vam pomoći u postavljanju i održavanju ovih parametara te u skladu s tim pohranjivati podatke.

Pohrana podataka: što i koliko dugo?

Kada pokušavate riješiti određeni problem, kao što je slučaj s našim gornjim primjerom osvjetljenja, morate razumjeti međusobnu korelaciju različitih skupova podataka.

Primjerice, trebaju vam **podaci u stvarnom vremenu** s IoT uređaja kako biste saznali jesu li svjetla uključena ili isključena. Također možete saznati je li soba prazna ili puna ili je prirodno svjetlo u sobi dovoljno samo za sebe. Te informacije pripadaju kratkotrajnom skladištu, gdje im se može lako pristupiti.

Također vam je potreban pristup nekim **istorijskim podacima** koji će vam pomoći da uočite obrasce.

Kad ste prije šest mjeseci eksperimentirali s automatskim mjeračima vremena na svjetlima, kakav je utjecaj imao na vaše troškove energije? Kada je vaš objekat najviše zauzet, a kada mirna razdoblja? Je li ova promjena sezonska? Zavisno o vašoj djelatnosti, možda ćete htjeti zaroniti u ove podatkovne tačke svakih nekoliko mjeseci. Stoga ih ima smisla pohraniti u dugoročno skladište analitike. Tamo su troškovi niži od kratkoročnih pogodnosti.

Koristite analitiku za dobijanje potpune slike

Izvođenje napredne analitike na **podacima u stvarnom vremenu i na istorijskim podacima** znači da možete cjelovitije razumjeti kako se vaš objekat ponaša po pitanju potrošnje energije na osvjetljenje. Omogućuje vam i proaktivno provođenje rješenja prije nego što se pojave problemi.

Podijelom podataka na ovaj način dobivate i najbolje od oba svijeta. Kako povezujete svoje uređaje, vaši IoT podaci dolaze u kratkotrajno skladište. Eto, imate brzinu i performanse potrebne za obradu ovih podataka u stvarnom vremenu. Ostali, manje neposredni podaci mogu se dugoročno pohraniti, s većim kapacitetom i pod manjom cijenom.

Platformu razmotrite i kao dio svoje podatkovne strategije

Kada razvijate slučaj upotrebe vašeg IoT projekta, morate razmotriti strategiju podataka. To uključuje i odabir prave platforme. Trebate rješenje koje vam omogućuje optimizaciju pohrane podataka, a mi preporučujemo pronalaženje partnera s višeslojnim pristupom podacima. Na taj način možete optimizirati troškove i postići bolji povrat ulaganja u IoT.

Četiri koraka za dobivanje najveće vrijednosti iz IoT podataka

Daleko ste odmakli na vašem IoT putovanju. To putovanje je posebno zanimljivo, ne samo što je ioT jako zanimljiva tema, već I zato što se i IoT nalaze u snažnoj fazi razvoja ka zreloj tehnologiji. Upravo zbog toga to putovanje je jako zanimljivo.

Izvlačenje vrijednosti iz podataka je specijalizovana oblast informacijskih tehnologija koja je izuzetno razvijena I to je jedna od ključnih tehnologija koje kompanije nastoje iskorstiti u digitalnoj transformaciji svog poslovanja. (O ovoj oblasti AITI ima posebno razvijen kurs: Upravljanje I analitika podataka).

Zbog svoje specifičnosti po pitanju količine I brzine prikuljanja podataka, tehnike izvlačenja vrijednosti iz podataka u IoT tehnologiji predstavlja poseban izazov.

Pogledajmo četiri koraka koje svaka organizacija treba svladati da bi uistinu shvatila vrijednost svojih IoT napora.

Korak 1: Prikupljanje podataka

Korak 1 započinje s osnovama: IoT podacima.

Ili preciznije, prikupljanje podataka sa svojih uređaja u upotrebljiv format.

Kad se IoT prvi put pojavio na sceni, bili smo fascinirani onim što smo mogli raditi u svojim domovima. Otkrili smo da možemo povezati stvari - poput naših sijalica - s IoT.

I tu bismo vezu mogli iskoristiti za njihovo isključivanje i uključivanje.

Super tehnologija, a te rane veze stvorile su veliku pompu. Ali s kojim ciljem?

Zato 1. korak započinje s osnovama: IoT podaci. Ili tačnije, prikupljanjem podataka sa IoT uređaja u upotrebljiv format.

Korak 2: Vizualizirajte uzorke

Kako je tehnologija sazrijevala, tako su rasla i očekivanja kompanija. Zbog toga se, kako se tržište razvijalo, fokus prebacio s instrumentiranja podataka na njihovu vizualizaciju.

Uzmimo tu povezanu sijalicu u koraku 1 i premjestimo je u veliko maloprodajno poduzeće. Ako ste sve što ste učinili bilo uključivanje i isključivanje mnogih sijalica putem njihovih senzora, onda da, to je prikladno. Ali je li korisno? Ili drugačije rečeno - je li dovoljno korisno opravdati pretvaranje svih vaših objekata s instrumentiranim sijalicama?

Još je zanimljivije - i korisnije - što nam povezana sijalica može reći o načinu na koji se koristi. Ti uvidi pokazuju vam potrošnju energije. Oni pomažu vlasniku maloprodaje u upravljanju potrošnjom energije i razumiju gdje i kako uštedjeti novac i resurse.

Na primjer, možda postoje područja koja u određeno vrijeme ne moraju biti osvijetljena. Ili otkrijete da u posebno sunčanim danima možete prigušiti svjetla za 10 posto i pritom zadržati istu razinu svjetline. Kad jednom počnete razumjeti obrasce u svojim podacima, a zatim primijenite vrijednost na svoje poslovanje, iskoristite korak 2 maksimalno.

Korak 3: Usmjerite se prema analitici

Sljedeći korak u IoT putovanju usredotočen je na to da podatke učinimo još pametnijima pomoću analitike.

Analitika vam omogućuje spajanje podataka IoT uređaja u stvarnom vremenu s postojećim, dugoročnim i istorijskim informacijama.

To vam omogućava da dobijete potpuniju sliku onoga što se događa s vašim uređajima i u vašem okruženju. Također vam omogućuje uočavanje obrazaca i predviđanje te usvajanje novih praksi koje proaktivno izbjegavaju rizik i izbjegavaju potencijalne probleme.

Da bismo ilustrirali, promijenimo primjer od povezanih sijalica do sofisticiranijih proizvodnih mašina. Povremeno jedna od tih mašina otkaže kada dođe do zastoja rada elektronike. Ali samo ponekad. Tu vam analitika može pomoći da glumite detektiva da biste riješili problem. Pregledom ostalih podataka otkrivate da vaši temperaturni senzori bilježe skok dva sata prije zakazivanja elektronike. Kad se te dvije stvari dogode, veća je vjerojatnost da će elektronika vaše mašine otkazati. Sada, s informacijama iz više izvora, možete sigurnije predvidjeti određenu kombinaciju faktora koji uzrokuju probleme. To zauzvrat omogućuje poduzimanje proaktivnijih mjera kako bi mašine ostale u pogonu, smanjujući vrijeme zastoja i povećavajući produktivnost.

Korak 4: Dodajte umjetnu inteligenciju

Četvrti korak na IoT putovanju usredotočen je na korištenje umjetne inteligencije kako biste učinili još više s vašim podacima.

Čak i uz profinjenu primjenu kako IoT može pomoći vašem poslovanju, i dalje ćete imati previše podataka, pogotovo dok kombinirate skupove podataka.

Lako možete doći u situaciju da budete zatrpani podacima, I jedino rješenje u tom slučaju jested a koristite AI.

Machine learning pomoći će vam očistiti podatke koje imate, razvrstati ih na najrelevantnije dijelove i pronaći naizgled očajne skupove podataka koji su zapravo važni.

Tim ćete naporima pronaći još više sinergije u svojim podacima.

Također pomaže prepoznati koje podatke treba koristiti, a što izbaciti, jer svi podaci nisu jednaki. Kako budete usavršavali postupak, moći ćete obavljati sofisticiranije zadatke poput modela predviđanja, primijeniti predviđajuće održavanje i otkrivanje anomalija. Drugim riječima, stječete pravi, bogati kontekst koji pomaže razumjeti ono što vidite. Moći ćete i lakše rješavati probleme, a možda čak i prepoznati nove mogućnosti i poslovne modele.

Nadamo se das mo vam ukratko objasnili zbog čega je ključ uspjeha vašeg IoT projekta u tome dag a napravite inteligentnim.

U narednoj sekciji ćemo vam pokazati kako ovu teoriju pretvoriti u praksu.

2. Razvoj inteligentne IoT aplikacije

Prospekt inteligentnih IoT uređaja;

Prikupljanje, vizualiziranje, analiziranje i otkritivanje anomalije u IoT podacima

U ovoj sekciji ćemo vas provesti kroz postavljanje IoT uređaja, prikupljanje podataka na platformi Watson IoT, istraživanje podataka i stvaranje vizualizacija, a zatim korištenje naprednih usluga Machine learning za analizu podataka i otkrivanje anomalija u istorijskim podacima.

Kako započeti

U predhodnom poglavlju smo vam pokazali kako da registrirate i povežite svoj uređaj, bilo da je to senzor, pristupnik ili nešto drugo, na Watson IoT Platformu i kako da počnete sigurno slati podatke u Cloud pomoću otvorenog, laganog MQTT protokola za razmjenu poruka.

Uređaje možete postaviti i upravljati njima putem mrežne nadzorne ploče ili IBM sigurnih API-ja, tako da vaše aplikacije mogu pristupiti vašim aktivnim i istorijskim podacima.

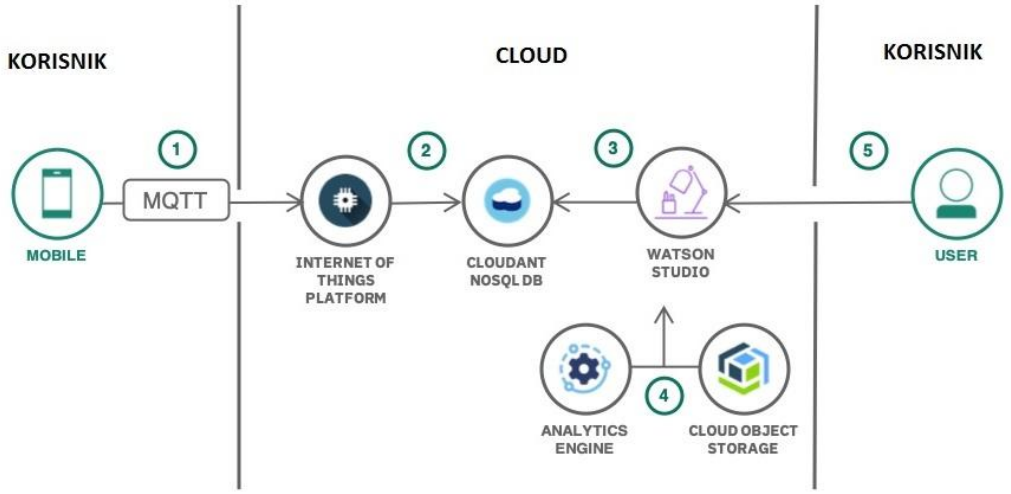
IBM Watson ™ Studio pruža vam okruženje i alate za rješavanje vaših poslovnih problema zajedničkom radom s podacima. Možete odabrati alate koji su vam potrebni za analizu i vizualizaciju podataka, za čišćenje i oblikovanje podataka, za unos podataka o strujanju ili za stvaranje i obuku modela strojnog učenja.

Ciljevi

Ciljevi ovog projekta su:

- Postavite IoT Simulator za prikupljanje podataka senzora mobilnih uređaja.
- Pošaljite prikupljene podatke na platformu Watson IoT.
- Stvorite vizualizacije s Jupyterovom bilježnicom.
- Analizirajte podatke generirane na uređaju i otkrijte anomalije.

Prikaz: Arhitektura inteligentne IoT aplikacije sa Watson IoT



Legenda:

1. Korisnik premješta mobilni uređaj za generiranje i slanje podataka senzora na IBM Watson ™ IoT platformu pomoću MQTT protokola.
2. Istorijski podaci senzora zatim se prenose u bazu podataka IBM Cloudant.
3. Watson ™ Studio povlači podatke iz baze podataka IBM Cloudant.
4. Podaci se analiziraju i vizualiziraju putem Jupyterove bilježnice u Watson™ Studio.
5. Korisnik sada može vidjeti vizualizacije i provjeriti anomalije u podacima senzora.

Prije nego što počnete:

Ova lekcija zahtjeva da imate:

- IBM Cloud CLI,
- i git za kloniranje spremišta izvornog koda.

Korak 1: Kreirajte IoT platformu

Za početak ćete kreirati uslugu Internet of Things Platform - čvorište koje može upravljati uređajima, sigurno se povezivati i prikupljati podatke te povijesne podatke učiniti dostupnima za vizualizacije i aplikacije. To može biti projekat sličan projektu koji ste razvili u predhodnom poglavlju.

Za ovaj zadatak trebaće vam novi projekat, zbog čega ćemo ponoviti korake koje je potrebno da poduzmete:

1. Idite na IBM Cloud Catalog i odaberite Platforma Internet of Things u odjeljku Internet of Things.
2. Odaberite regiju i odaberite Lite kao cjenovni plan.
3. Unesite **`IoT demo hub`** kao naziv usluge.
4. Kliknite **Create**, a zatim **Lounch** (pod Upravljanje) u nadzornoj ploči (Dashboard).
5. Na bočnom meniju odaberite **Security** > kliknite ikonu **Edit** pored **Connection Security** i odaberite **TLS Optional** pod **Default Rule** > **Security Level** i kliknite **Save**.
6. Na bočnom meniju odaberite **Device** > **Device Type** i onda kliknite **Add Device Type**.
7. Unesite **`simulator`** kao **Name** i kliknite **Next** i **Finish**.
8. Zatim kliknite **Register Devices**.
9. Odaberite **simulator** kao **Device Type** i unesite **`telefon`** za **Device ID**.
10. Kliknite **Next** dok se ne prikaže displej **Security**.
11. Unesite vrijednost za **Authentication Token**, na primjer: **`myauthtoken`** i kliknite **Next**.
12. Nakon što kliknete **Finish**, prikazuju se podaci o vašoj vezi. Neka ta kartica ostane otvorena.

IoT platforma je sada konfigurirana za početak primanja podataka. Uređaji će trebati poslati svoje podatke na IoT platformu s navedenim vrstom uređaja, ID-om i tokenom.

Korak 2: Izradite simulator uređaja

U drugom koraku vi trebate instalirati node.js web aplikaciju.

U ovom koraku ćemo vam samo predstaviti kako se to radi sa unaprijed pripremljenim kodom, obzirom da AITI ima poseban kurs koji vam može pomoći da savladate programiranje u Node.js.

Cilj ovog koraka je da pokrenete Node.js aplikaciju na vašem telefonu, koja će se povezati i poslati podatke o akcelerometru i orijentaciji uređaja na IoT platformu.

To možete uraditi na slijedeći način:

1. Klonirajte spremište Github:

   ```
   $ git clone https://github.com/IBM-Cloud/iot-device-phone-simulator
   ```

```
cd iot-device-phone-simulaor
```

2. Gurnite (eng. Push) aplikaciju u IBM Cloud pomoću slijedeće instrukcije:

```
$ibmcloud login
ibmcloud target --cf
ibmcloud cf push
```

3. Za nekoliko minuta vaša će aplikacija biti postavljena i trebali biste vidjeti URL sličan **`<random-name>.mybluemix.net`**

4. Posjetite URL aplikacije s HTTPS-om (**`https://<random-name>.mybluemix.net`**) na svom telefonu pomoću internet pretraživaća.

5. Unesite podatke o vezi s kartice IoT Dashboard u odjeljku **Device Credentials** i kliknite **Connect**. Vrijednosti veze trebaju izgledati slično parametrima prikazanim u donjoj tabeli.

   Tabela: Podaci o konekciji

Parametar	Vrijednost
Organization ID	Pronađi vrijjednost pod vašim USER NAME na VRHU trake
Device Type	Simulator
Device ID	telefon
Authentication Token	Simulator

   Savjet: Na iOS-u 13.x ako se to zatraži, dopustite web lokaciji pristup podacima senzora pokreta i orijentacije. Na iOS-u 12.x pristup senzorima je prema zadanim postavkama onemogućen u Safariju. Da biste ručno omogućili, otvorite Postavke -> Safari -> Motion & Orientation access.

6. Vaš će telefon početi prenositi podatke. Potražite nove unose u odjeljku **Recent Events**.

Korak 3: Prikažite podatke uživo u IBM Watson IoT platformi

Zatim ćete stvoriti ploču i kartice za prikaz podataka uređaja na nadzornoj ploči.

To možete uraditi sa dva podkoraka gdje će te u prvom kreirati novu Ploču (eng. Create a Board), a u drugom prikazati podatke sa uređaja (eng. Display device data).

Kreirajte ploču:

1. Odaberite ploče s lijevog menija, a zatim kliknite **Create New Board**.
2. Unesite naziv ploče, **`Simulatori`** kao primjer i kliknite **Next**, a zatim **Submit**.
3. Odaberite ploču koju ste upravo stvorili da biste je otvorili.

Prikaz podataka uređaja:

1. Kliknite **Add New Card**, a zatim odaberite vrstu kartice **Line Chart** koja se nalazi u **Device section**.
2. Odaberite svoj uređaj s popisa, a zatim kliknite **Next**.
3. Kliknite **Connect new data set**.
4. Na stranici **Create Value Card page** odaberite ili unesite sljedeće vrijednosti i kliknite **Next**.
   - `Event: sensorData`
   - `Property: ob`
   - `Name: OrientationBeta`
   - `Type: Float`
   - `Unit: °`
   - `Precision: 1`
   - `Min: -180`
   - `Max: 180`
5. Na stranici **Card Preview page** odaberite **L** za veličinu linijskog grafikona i kliknite **Next** > **Submit**
6. Kartica se pojavljuje na nadzornoj ploči i uključuje linijski grafikon podataka **`OrientationBeta(ob)`** uživo.
7. Upotrijebite internet pretraživač svog mobilnog telefona za ponovno pokretanje simulatora i polako naginjanje telefona naprijed i natrag.
8. Natrag na kartici **IBM Watson IoT Platform Boards** trebali biste vidjeti kako se grafikon ažurira.

Korak 4: Pohranite istorijske podatke u IBM Cloudant

U ovom ćete koraku stvoriti **IBM Cloudant** uslugu i povezati je s Watson IoT Platformom za pohranu istorijskih podataka.

Prvi podkorak u ovom procesu jeste da kreirate **IBM Cloudant DB** i da se povežite sa aplikacijom na slijedeći način:

1. Idite na **IBM Cloud Catalog** i izradite novu instancu **IBM Cloudant**:
   - U odjeljku **Select an environment** ostavite **Multitenant** i odaberite regiju
   - Unesite `iot-db` kao ime instance
   - Kao način provjere autentičnosti odaberite **both legacy credentials and AIM**
   - Odaberite **Lite** plan i kliknite **Create**.
2. Idite na **Resource list** i unesite `iot-db` u polje **Name** da biste provjerili status usluge. Kad se status promijeni u **Provisioned**, kliknite naziv usluge da biste vidjeli stranicu **Manage page**.
   - Na lijevom meniju kliknite **Service credentials**.
   - Kliknite **New credentials**, a zatim **Add**
   - Proširite novostvorene vjerodajnice i spremite ih za buduću upotrebu.
3. Pod **Conncections**:
   - Kliknite **Create connections**
   - Odaberite mjesto, organizaciju i proctor u **Cloud Foundry** gdje trebate kreirati alias za **IBM Cloudant** uslugu.
   - Proširite naziv prostora u tabeli **Location Connection** i upotrijebite dugme **Connect** pored **iot-solution-tutorial** kako biste stvorili alias za uslugu IBM Cloudant u tom prostoru.
   - Povežite i ponovo pokrenite aplikaciju pritiskom na **Connect**.

Drugi korak je da kreirate data connector za pohranu istorijskih podataka. To možete uraditi postavljanjem nove konekcije u četri podkoraka:

- Stvorite obvezujuću uslugu koja pruža Watson IoT Platformi potrebne informacije za povezivanje s uslugom Cloudant.
- Stvorite instancu konektora za vezivanje usluge.
- Konfigurirajte jedno ili više odredišta na konektoru.
- Postavite jedno ili više pravila prosljeđivanja za svako odredište.

Da biste postavili novu vezu, potrebno je:

1. Na nadzornoj ploči Watson IoT Platforme kliknite ikonu **Watson IoT Platform Help** (ikona pomoći na traci izbornika) na gornjoj traci, kliknite **API**, a zatim **View APIs** pored **Historian Connector** da biste vidjeli interaktivne API dokumente.

2. Pod **Services** proširite krajnju točku **POST/s2s/services** i kliknite **Try it out**. Zamijenite rezervirana mjesta u JSON-u ispod sa *cloudanet service credentials* i upotrijebite ih kao sadržaj za **Example Value** u tijelu **Service**.

```
{
   "name": "iot-cloudant",
   "type": "cloudant",
   "description": "for IoT solution tutorial",
   "credentials": {
     "username": "CLOUDANT_USERNAME",
     "password": "CLOUDANT_PASSWORD",
     "host": "CLOUDANT_HOST",
     "port": 443,
     "url": "CLOUDANT_URL"
   }
 }
```

3. Kliknite **Execute** da biste vidjeli odgovor **`HTTP 201`**. Spremite **`id`** (serviceID) iz odgovora za sljedeći API call.

4. U odjeljku **HistorianConnectors** proširite krajnju točku **POST/historianconnectors** i kliknite **Try it out**. Zamijenite **Example Value** ispod tijela konektora s donjim JSON-om kodom. Ne zaboravite zamijeniti **`SERVICE_ID`** ID-om iz gornjeg odgovora.

```
{
   "name": "iot-cloudant-connector",
   "description": "Historian connector connecting IoT platform to cloudant",
   "serviceId": "SERVICE_ID",
   "type": "cloudant",
   "enabled": true
 }
```

5. Kliknite Izvrši da biste vidjeli odgovor HTTP 201. Spremite id (connectorID) iz odgovora za buduću referencu.

6. U odjeljku Odredišta proširite krajnju točku **POST /historianconnectors/{connectorId}/destinations** i kliknite **Try it out**. Navedite **`id`** (connectorID) i zamijenite **Example Value** pod **Destination** s JSON-om kodom ispod:

```
{
 "name": "default",
 "type": "cloudant",
 "configuration": {
   "bucketInterval": "DAY"
  }
}
```

7. Kliknite **Execute** da biste vidjeli odgovor **`HTTP 201`**.

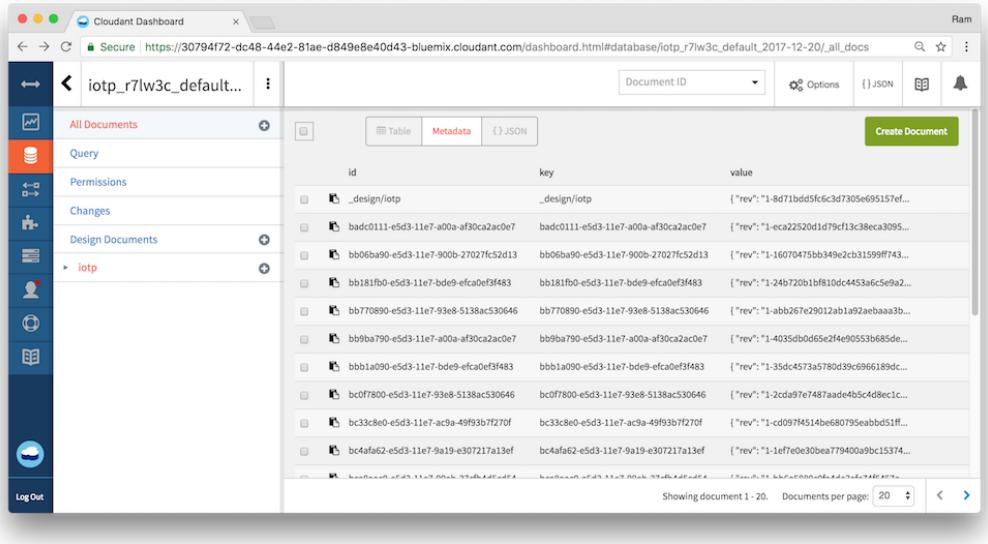
8. Pod **Forwarding Rules** proširite krajnju točku **POST /historianconnectors/ {connectorId}/forwardingrules** i kliknite **Try it out**. Navedite **`id`** (connectorID) i zamijenite **Example Value** u tijelu **Forwarding Rule** s JSON-om kodom ispod:

```
{
 "name": "iot-cloudant-rule",
 "destinationName": "default",
 "type": "event",
 "selector": {
   "deviceType": "simulator",
   "eventId": "sensorData"
  }
 }
```

9. Kliknite **Execute** da biste vidjeli odgovor **`HTTP 201`**.

Savjet: Korištenjem Python SDK-a možete postaviti vezanje Cloudant NoSQL DB-a u samo nekoliko redaka koda. Za više informacija o tome kako proslijediti IoT podatke u Cloudant NoSQL DB, provjerite **configuration section** u dokumentaciji konektora podataka.

Podaci vašeg uređaja sada će se spremiti u IBM Cloudant. Ponovno povežite aplikaciju preglednika da biste generirali nove podatke. Nakon nekoliko minuta pokrenite nadzornu ploču IBM Cloudant da biste vidjeli svoje podatke.



Korak 5: Otkrivanje anomalija pomoću Machine learning

U ovom koraku imaćete priliku da se upoznate sa moćima koje donosi vještačka inteligencija. Machine learning je jako sofisticirana tehnologija koja je neizostavna u savremenom radu sa velikim količinama podataka.

U ovom priručniku mi se nečemo duboko posvećivati ovoj temi, a podsjećamo das mo već rekli da AITI ima poseban trening path koji je usmjeren na razvoju kapaciteta u oblasti data management and analytics, gdje svi vi koji ste zainteresovani možete naučiti puno toga o ovoj oblasti. Tu možete naučiti puno više o alatima kao što su Node, Spark, Hadoop i slično.

U ovom koraku ćete naučiti koristiti Jupyter Notebook koja je dostupna u usluzi IBM Watson ™ Studio za učitavanje vaših istorijskih mobilnih podataka i otkrivanje anomalija korištenjem z-score. Z-score statistilčka tehnika koja vam pomaže da saznate standardni rezultat koji pokazuje koliko je elementarnih odstupanja element od srednje vrijednosti.

Pa krenimo tako što ćemo kreirati novi projekat

1. Idite na **IBM Cloud Catalog** i pod **AI** odaberite **Watson ™ Studio**.
2. Kreirajte uslugu klkanjem na **Create**:
   - Odaberite regiju i odaberite **Lite** cjenovni plan

- Unesite **Service name** i odaberite grupu resursa

3. Pokrenite nadzornu ploču klikom na **Get Started** i kliknite Create project > Kreirajte prazan projekt i unesite `Detect anomaly` kao **Name** projekta.
4. Ostavite neoznačen potvrdni okvir **Restricted who can be a collaborator** jer nema povjerljivih podataka.
5. Odaberite postojeću uslugu **Cloud Object Storage** u odjeljku **Define Storage** ili izradite novu (odaberite **Lite** plan> **Create**). Pritisnite **Refresh** da biste vidjeli kreiranu uslugu.
6. Kliknite **Create**. Otvara se vaš novi projekt i možete mu početi dodavati resurse.

Odlično.

Sada idemo dalje.

Naredni korak je da se povežemo sa bazom podataka

Veza s IBM Cloudantom za podatke:

1. Kliknite + **Add to project** > **Connection**
2. Odaberite **iot-db** IBM Cloudant u kojem su pohranjeni podaci uređaja.
3. Potvrdite **Credentials**, a zatim kliknite **Create**.

Super. To je to. Sada idemo da razvijemo analitičku mašinu.

Ako nemate postojeću uslugu **IBM Analytics Engine**:

1. Idite na IBM Cloud katalog i odaberite **Analytics Engine**
2. Odaberite regiju i odaberite **Lite** plan
3. Unesite naziv usluge, odaberite grupu resursa i kliknite **Configure**.
4. Na stranici za konfiguraciju postavite Softverski paket na **AE 1.2 Spark and Hadoop** i kliknite **Create**.

Jednom kada usluga bude omogućena ili ako imate postojeću instancu usluge koju želite koristiti i konfigurirati sa softverskim paketom **AE 1.2 Spark and Hadoop**:

1. Iz liste **Resource list** otvorite kreiranu uslugu.
2. U odjeljku **Service credentials** kreirajte nove vjerodajnice:
   - Postavite **Name** na **wdp –writer**
   - Postavite **Role** na **Writer** i kliknite **Add**

3. U odjeljku **Manage** dohvatite korisničko ime i lozinku za klaster. Možda ćete trebati resetirati lozinku klastera.

U Watson Studio:

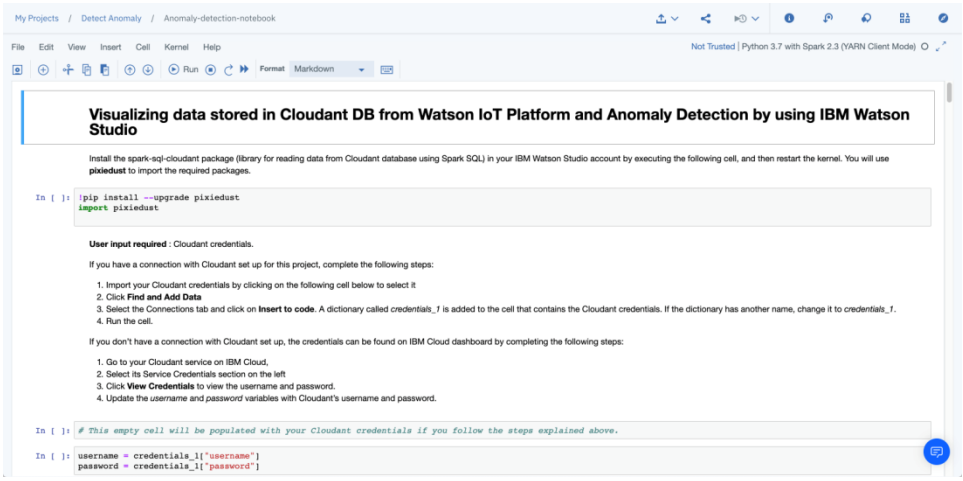
1. Odaberite projekt **Detect Anomaly**.
2. Kliknite **Settings** na gornjoj navigacijskoj traci.
3. Pomaknite se do **Associated Services**.
   - Kliknite **Add service**.
   - Odaberite **IBM Analytics Engine**.
4. Kliknite instancu **Existing** uslugu.
5. Unesite korisničko ime i lozinku klastera.
6. Pritisnite **Select**.

Sada je potrebno da kreirate Jupyterovu (ipynb) Notebook (bilježnicu)

1. Kliknite **+ Add to Project** i dodajte novi **Notebook**.
2. Odaberite **Form URL** I unesite **`Anomaly-detection-notebook`** kao vaš Notebook **Name**.
3. Unesite

   `https://github.com/IBM-Cloud/iot-device-phone-simulator/raw/master/anomaly-detection/Anomaly-detection-watson-studio-python3.ipynb`

   u **Notebook URL**.
4. Odaberite uslugu **IBM Analytics Engine** pridruženu u gornjem koraku kao vrijeme izvođenja (eng. runtime).
5. Kreirajte **Notebook**.
6. Postavite **`Python 3.7 with Spark 2.3 (YARN Client Mode)`** kao vaš Kernel. Provjerite je li bilježnica kreirana s metapodacima i kodom.



Da bi ažurirali, **Kernel**> **Change kernel**. Da biste vjerovali bilježnici, **File** > **Trust Notebook**.

Sada je vrijeme da detektujete anomalije.

Pokrenite Notebook.

1. Odaberite ćeliju koja započinje sa `!Pip install --upgrade pixiedust`, a zatim kliknite **Run** ili **Ctrl + Enter** da biste izvršili kôd.

2. Kada je instalacija završena, ponovno pokrenite Spark kernel klikom na ikonu **Restart Kernel**.

3. U sljedeću ćeliju koda, importujte svoje vjerodajnice za IBM Cloudant u tu ćeliju tako što ćete izvršiti sljedeće korake:

   - Kliknite

   - Odaberite karticu **Connection**.

   - Kliknite **Insert to code** > Insert Credentials. Rječnik nazvan `_credentials1` kreira se s vašim vjerodajnicama IBM Cloudant. Ako ime nije navedeno kao `_credentials1`, preimenujte rječnik u `credentials_1` `credentials_1` će se koristiti u preostalim ćelijama.

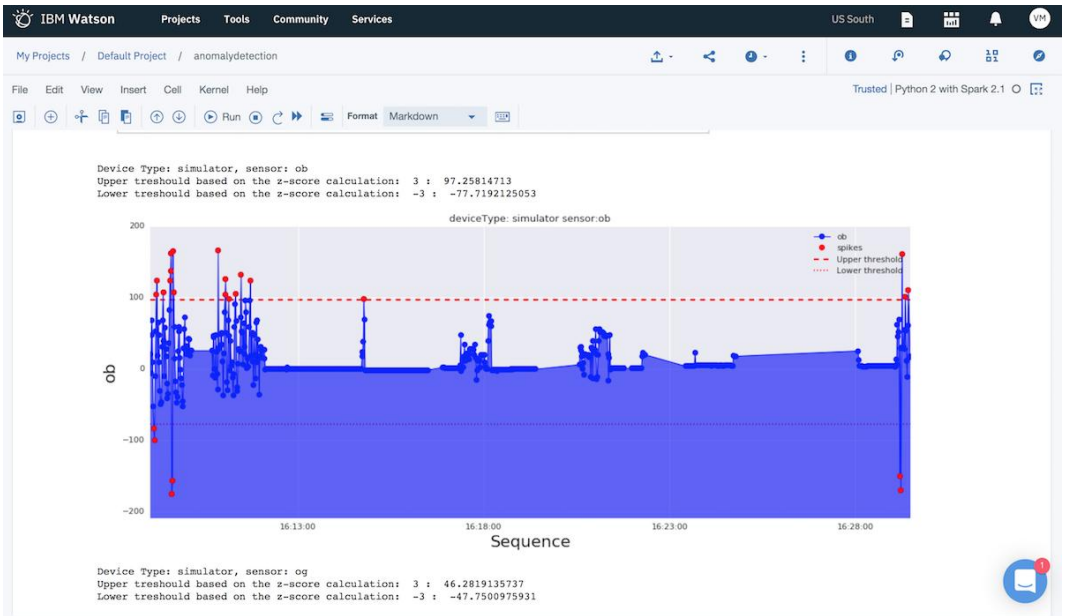
4. U ćeliju s imenom baze podataka (`dbName`) unesite ime baze podataka IBM Cloudant koja je izvor podataka, na primjer, `iotp_yourWatsonIoTProgId_DBName_Year-month-day`.

   Da biste vizualizirali podatke različitih uređaja, promijenite vrijednosti `deviceId` i `deviceType` u skladu s tim. Tačnu bazu podataka možete pronaći tako da

prijeđete na vašu instancu **iot-db** IBM Cloudant koju ste ranije kreirali > **Launch Dashboard**.

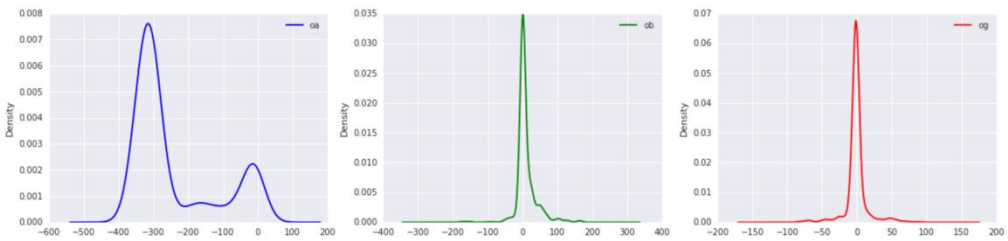
5. Spremite notebook i izvedite svaku ćeliju koda jednu za drugom ili pokrenite sve (**Cell** > **Run All**), a na kraju nootebook trebali biste vidjeti anomalije podataka o kretanju uređaja (oa, ob i og). Vremenski interval od interesa možete promijeniti u željeno doba dana. Potražite `start` i `end` vrijednost.

Jupyter Bilježnica DSX



6. Uz otkrivanje anomalija, ključni nalazi ili izvori iz ovog odjeljka su:

- Upotreba **Spark** za pripremu podataka za vizualizaciju.
- Korištenje **Pandas** za vizualizaciju podataka
- Trakasti grafikoni, histogrami podataka uređaja.
- Korelacija između dva senzora kroz matricu korelacije.
- Grafički prikaz za svaki senzor uređaja, proizveden s funkcijom Pandas plot.
- Grafikoni gustoće kroz Kernel density estimation (KDE).



Korak 6: Uklonite resurse

7. Idite na **Resource List** > odaberite **Location**, **Org** i **Space** na kojem ste kreirali aplikaciju i usluge. U odjeljku **Cloud Foundry Apps** izbrišite aplikaciju **Node.JS** koju ste prethodno kreirali.
8. U odjeljku **Service** izbrišite odgovarajuće IBM Watson ™ IoT platforme, IBM Analytics Engine, IBM Cloudant i IBM Cloud Object Storage usluge koje ste kreirali za ovu vježbu.

Čestitamo.

Primjena kognitivnih tehnologija – kreraj TJBot robota

Došli smo do skoro samog kraja.

Do sada ste imali prilike da se upoznate sa osnovama IoT tehnologija i hardveru koji se koristi, komunikacijskim tehnologijama na kojima počivaju povezani uređaji te pristupima u dizajniranju apllikacija koje upravljaju IoT uređajima.

Nakon toga ste imali priliku da se malo dublje upoznate sa pitanjem sigurnosti koje će uvijek biti izuzetno važno pitanje koje treba razmotriti kada razvijate IoT projekat.

Ovaj priručnik je namjenjen da vas uvede u svijet inteligentnih IoT uređaja. Zbog toga smo ovo posljednje poglavlje rezervisali za ključne karakteristike IoT tehnologija od kojih zavisi stepen inteligencije vašeg IoT projekta. Tu smo vam nastojali približiti važnost upravljanja podacima koje generišu IoT uređaji I ulogu napredne analitike koju pokreće vještačka inteligencija.

Naše je mišljenje da je ovo sasvim dovoljno da samostalno krenete u istraživanje svijeta povezanih uređaja.

Ali kao što smo rekli došli ste do samog kraja.

Prije nego što završimo, planirali smo za vas još jednu sekciju u kojoj ćemo nastojati obuhvatiti sve što ste do sada mogli naučiti I svo znanje podići za još jednu ljestvicu.

Za to postoji vrlo dobar razlog.

Vi ste do sada imali prilike da se upoznate sa brojnim hardverskim I softverskim komponentama koje se mogu koristiti za IoT projekat.

Pokazali smo vam kako se sa njima mogu napraviti tradicionalni IoT projekti ali i kako se sve te komponente mogu iskoristiti za pravi inteligentni projektat. Upoznali ste kako se može iskoristiti Raspberry Pi, mikrofoni, senzori, zvučnici, dodaci, sijalice, kamera koji mogu pomoći da bilo koja stvar bude povezana na internet.

Naravno da to nije sve što mogu ponuditi IoT tehnologije, pogotovo što se one svakodnevno razvijaju I još su jako doleko od toga da ih možemo smatrati zrelim tehnologijama.

Ali sigurno se neki od vas može zapitati koliko daleko se mogu razvijati IoT tehnologije.

Zahvaljujući kognitivnim tehnologijama I vještačkoj inteligenciji vi možete ne samo povezati svari već i oživiti.

Mi smo sa jasnom namjerom u ovom priručniku odabrali da vas upoznamo dublje sa IBM Watson IoT iz jednog jedinog razloga: IBM Watson je kognitivni kompjuter koji je dizajniran za za primjenu naprednog procesiranja naturalnog jezika, korištenje informacija, reprezentaciju znanja, automatsko rezonovanje I machine learning tehnologije.

I vi ste već koristili Watsona u tri predhodna projekta koje ste uspješno završili.

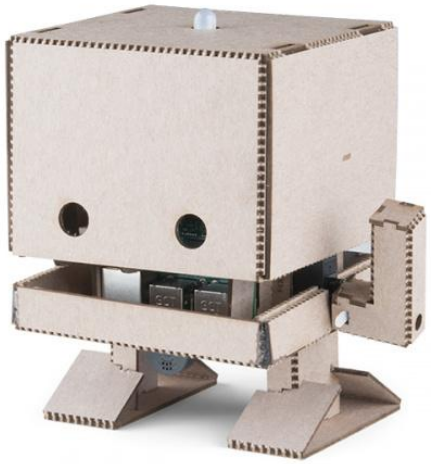
Sada, pomoću IBM Watson i IoT Starter Kits krenimo zajedno da povežemo sve te IoT gadgets u programiranog robota koji je izuzetno inteligentan.

Kranimo.

Uvod

Vi imate zadatak da napravite IoT uređaj koji je jako inteligentan – TJ Bot-a.

TJBot je komplet razvijen u IBM-u kako bi pomogao ljudima da započnu sa svojom Watson AI uslugom. Dolazi s ljubaznim malim robotom kojeg sami gradite, Raspberry Pi 3, i svim dijelovima koji su vam potrebni da vaš robot maše, trepće, razgovara i sluša.



Za to su vam potrebni slijedeći alati:

- USB Miš
- USB tastatura
- HDMI monitor
- 5V napajanje
- IBM TJ Bot Maker Kit
- Priključak na internet

Instalacija

Prije nego što učinite bilo što drugo, preporučujemo da postavite Raspberry Pi, povežete ga s Internetom i ažurirate OS. Ovdje ćemo vam pomoći u tome.

Uz minimalno postavljanje, Raspberry Pi 3 možete pokrenuti spajanjem PWR IN priključka mikro USB-a s USB priključkom računala. Međutim, preporučujemo da potražite ovo napajanje za zidni adapter za napajanje - 5,1 V DC 2,5 A (USB Micro-B).

Povežite monitor, tastaturu i miš kao što biste to učinili s bilo kojim računarom. Umetnite microSD karticu koju ste dobili s TJBot kompletom, a zatim uključite napajanje. Postoji samo jedno mjesto na koje se napajanje može fizički priključiti: mikro-B USB konektor s oznakom "PWR IN". Ponovno preporučujemo naš 5.1V Micro USB izvor napajanja za napajanje vašeg TJBot-a.

Na kartici **Keyboard** pronaći ćete gumb nazvan **Keyboard Layout**. Pronađite željeni raspored tipkovnice u prozoru koji će se pojaviti kad kliknete taj gumb.

Instalirajte TJBot

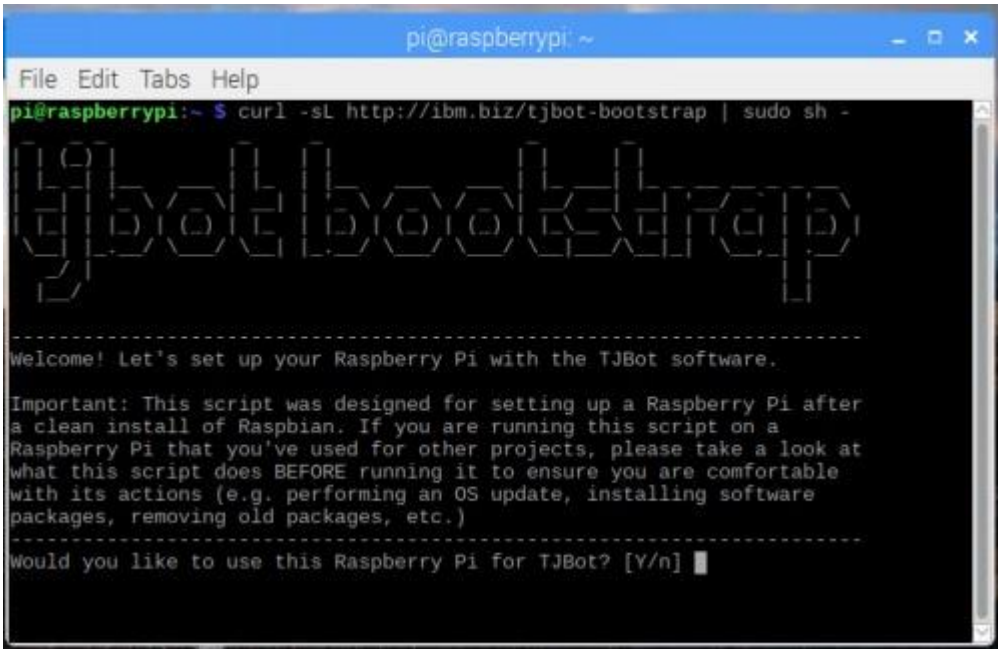
Instaliranje TJBot-a vrši se s jednom skriptom koja se može pokrenuti jednom naredbom. Naredba je:

```
curl -sL http://ibm.biz/tjbot-bootstrap | Sudo sh -
```

Kopirajte taj redak i zalijepite ga u prozor terminala. Otvorite prozor terminala klikom na gumb na traci na vrhu zaslona.

Napomena: Tipkovni prečac za kopiranje istaknutog teksta je ctrl + c. Međutim, ovo je drugačije u prozorima terminala. Morali biste istovremeno držati shift + ctrl + c. Dakle, ako biste prečac na tipkovnici koristili za lijepljenje kopiranog teksta u prozor terminala, standardni ctrl + v neće raditi. Morali biste istodobno pritisnuti tri tipke shift + ctrl + v.

Nakon što zalijepite ovaj redak koda u prozor terminala, pritisnite tipku Enter na tipkovnici. To će povući najnoviju verziju skripte TJBot Bootstrap s Interneta. Dobit ćete prozor koji izgleda otprilike ovako:



Vjerojatno radite na Raspberry Pi-u na kojem želite instalirati TJBot, pa upišite **'y**', a zatim pritisnite **Enter**.

Od vas će se zatražiti da unesete ime za svoj TJBot. Slobodno imenujte TJBot kako god želite ili jednostavno pritisnite **Enter** da biste ga ostavili nepromijenjenim. Zapravo nema veze, obećavam.

Tada ćete biti upitani želite li onemogućiti ipV6. Ponovno upišite "**y**" i pritisnite **Enter**.

Sljedeće je pitanje treba li koristiti Googleove poslužitelje imena za ubrzavanje DNS upita. Ponovno pritisnite "**y**", a zatim **Enter**.

Zatim će vas skripta pitati želite li **force locale to US English (en-US)**. Na ovo pitanje možete odgovoriti sa **no**.

Nadogradite OS na Raspberry Pi

Sada biste trebali dobiti upit koji izgleda ovako:

```
pi@raspberrypi: ~
File  Edit  Tabs  Help
In some networking environments, disabling ipv6 may help your Pi get on
the network.
Disable ipv6? [y/N] y
Disabling ipv6
 ipv6.disable=1
ipv6 has been disabled. It will take effect after rebooting.

In some networking environments, using Google's nameservers may speed up
DNS queries.
Enable Google DNS? [y/N]: y
Adding Google DNS servers to /etc/resolv.conf

Force locale to US English (en-US)? [y/N] y
Forcing locale to en-US. Please ignore any errors below.
en_US.UTF-8 UTF-8
Generating locales (this might take a while)...
  en_GB.UTF-8... done
  en_US.UTF-8... done
Generation complete.

TJBot requires an up-to-date installation of your Raspberry Pi's operating
system software. If you have never done this before, it can take up to an
hour or longer.
Proceed with apt-get dist-upgrade? [Y/n]
```

Skripta postavlja pomalo zastrašujuće zvučno pitanje o nadogradnji operativnog sustava vašeg Raspberry Pi. Upozorava da bi to moglo potrajati sat vremena ili duže (GULP)!

Ne brinite, prema našem iskustvu potrebno je oko deset minuta ili manje, ovisno o brzini vaše internetske veze. U svakom slučaju, morat ćete ponovo upisati "y", a zatim pritisnite Enter kako biste započeli postupak ažuriranja. Pripazite na zaslon dok traje postupak nadogradnje, ali ne trebate ga pažljivo nadzirati jer je cijeli postupak nadogradnje automatski. Zaslon za zaslonom teksta pomicat će se tijekom ovog postupka i ne morate se brinuti ni o čemu.

Instalirajte Node.js

Nakon završetka postupka nadogradnje primit ćete ovaj upit koji će vas pitati o instaliranju novije verzije Node.js.

```
pi@raspberrypi: ~
File  Edit  Tabs  Help
   - SHA1:a4454015495f545881edd8fc32606e4af1917f73 [weak]
   - MD5Sum:92880edcfa1d425bb658b2261e71659c [weak]
   - Filesize:31752192 [weak]
  Last modification reported: Wed, 13 Sep 2017 15:15:52 +0000
Fetched 111 MB in 3min 43s (495 kB/s)
E: Failed to fetch http://archive.raspberrypi.org/debian/pool/main/s/scratch2/sc
ratch2_0.17_armhf.deb  Hash Sum mismatch
   Hashes of expected file:
    - SHA256:a0d5a1a78565aa4f3497986781fd45c9ccc9edfb4b964caf107c3467514b6f68
    - SHA1:b4274968418d77c45f4fffbea06e69add214e240 [weak]
    - MD5Sum:3552619d18f3ba94b0406baa277221d3 [weak]
    - Filesize:67803408 [weak]
   Hashes of received file:
    - SHA256:7b2b04bc4bc9315478ede56d404f8061d04ccc86d65758ad203632020c9c8203
    - SHA1:a4454015495f545881edd8fc32606e4af1917f73 [weak]
    - MD5Sum:92880edcfa1d425bb658b2261e71659c [weak]
    - Filesize:31752192 [weak]
   Last modification reported: Wed, 13 Sep 2017 15:15:52 +0000
E: Unable to fetch some archives, maybe run apt-get update or try with --fix-mis
sing?

Node.js version v4.8.2 is currently installed. We recommend installing
Node.js version 7 for Raspian 9 (stretch).
Would you like to install a newer version of Node.js? [Y/n]
```

Još jednom, odgovorite potvrdno na ovo pitanje. Odmah nakon odgovora da, bit ćete upitani koju verziju Node.js treba instalirati. Upišite '9', a zatim pritisnite Enter. Dobit ćete još nekoliko zaslona teksta dok skripta preuzme i instalira Node.js verzije 9 na vaš Raspberry Pi.

Nakon instaliranja Node.js skripta će pitati imate li instaliranu kameru.

Sljedeće se pitanje odnosi na "kloniranje" TJBot projekta i gdje to treba klonirati. Kloniranje u ovom slučaju zapravo znači samo preuzimanje. Zadana lokacija za preuzimanje je radna površina, što je jednako dobro mjesto kao i svako i bolje od mnogih. Zato samo pritisnite tipku **Enter** da biste TJBot projekt preuzeli na radnu površinu.

Sad ćete dobiti zaslon sa skriptom

Skripta će vas pitati "**Disable sound kernel modules?**" Kako komplet TJBot tvrtke SparkFun koristi audio priključak za izlaz zvuka umjesto opcija HDMI ili USB izlaza, ovdje ćete htjeti pritisnuti '**no**'. Ako na ovo pitanje odgovorite "**yes**", zvuk neće raditi na kasnijim TJBot projektima i bit ćete tužni.

Sada ćete biti tretirani ASCII umjetničkim prikazom lica TJBot-a, porukom da je postavljanje završeno i pozivom da pritisnete **Enter** za nastavak.

Samo naprijed i pritisnite **Enter**.

Sad ćete dobiti zaslon teksta o registraciji za Lite IBM Cloud, načinu prijave, stvaranju instanci usluga, dobivanju vjerodajnica i drugim stvarima!

Zasad to samo zanemarite.

Na kraju, pitati vas želite li pokrenuti testove hardvera. Predlažem da odgovorite "**no**" jer neke promjene koje smo napravili tijekom postupka instalacije mogu uzrokovati neuspjeh ovih testova iako ništa nije u redu.

Posljednje je pitanje: "**Do you want to reboot now?**" Možete odgovoriti sa "**yes**" za trenutno ponovno pokretanje ili "**no**" i ponovo pokrenuti sustav kasnije. Preporučujem da nastavite i odgovorite "**yes**".

Kreiranje IBM Cloud računa

Čarobne moći TJBot-a potječu iz Watsona, IBM-ove službe za umjetnu inteligenciju. Da biste koristili Watson, sada je potrebno da kreirate Lite račun IBM Cloud.

Sada ćemo vas provesti kroz registraciju za račun IBM Cloud.

Prvi je korak da se registrujete.

Nakon što se registrujete potrebno je da postavite svoj IBM Cloud.

1. Kreirajte organizaciju odabirom **Create organization**.
2. Kreirajte proctor odabirom **Create space**.

   Prostor vam pomaže da bolje upravljate pristupom i ovlaštenjima za set resursa, I mapiranje razvojnih faza kao što su dev, test, I produkcija.
3. Sad ćete biti obavješteni da možete krenuti porukom Good to Go!

   Pritisite dugme **I'm Ready**
4. Nakon što je vaš IBM Cloud postavljen pojaviće vam se vaš dashboard.

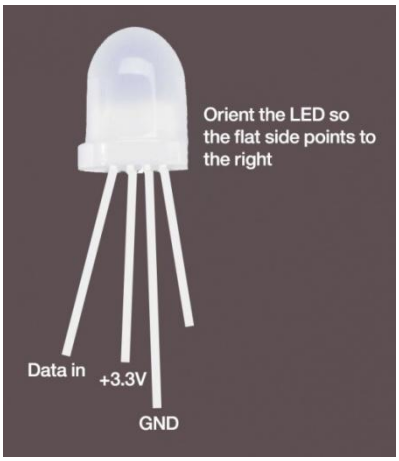
Sada ste spremni da krenete u razvoj TJBot-a.

Upravljanje glasom LED

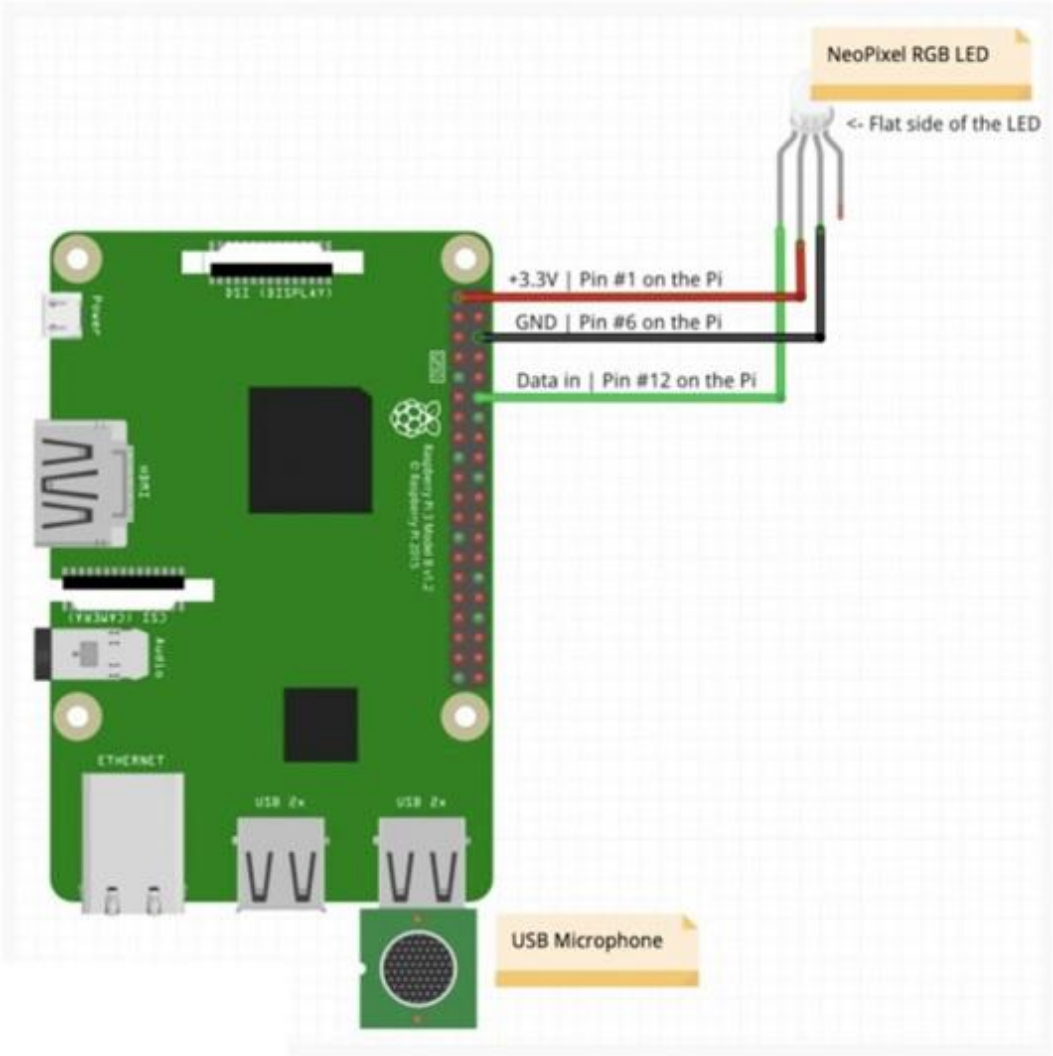
Naš prvi projekt je postaviti TJBot za glasovno upravljanje adresiranom LED diodom. Za početak moramo spojiti LED na TJBot.

LED priključak

Započnite s pronalaženjem jedne od LED dioda uključenih u TJBot komplet. Trebao bi izgledati poput donje slike i biti približno veličine gumice za olovke.



Sada ovu LED diodu morate povezati s Raspberry Pi. Pronađite žice kratkospojnika F / F koje su bile uključene u vaš komplet i slijedite donji dijagram kako biste spojili LED.



USB priključak mikrofona

Sada je vrijeme da USB mikrofon priključite u jedan od USB priključaka na Raspberry Pi. Nije važno u koji ga priključite priključak, samo ga priključite.

Postavite instancu govora u tekst na IBM Cloudu

Vratite se na nadzornu ploču IBM Cloud i kliknite na hamburger meni (Jeste li znali da se to naziva izbornikom hamburgera? Svaki dan učite nešto novo!) U gornjem lijevom kutu.

Iz lijevog ruba stranice iskočit će izbornik. Pronađite unos za "**Watson**" u ovom izborniku (nalazi se pri dnu i možda ćete ga trebati pomaknuti da biste ga pronašli) i kliknite na njega.

Reći će vam da još nemate nijedan primjerak usluge Watson i bit ćete pozvani da ga napravite. Kliknite dugme **Create Watson service**.

Otvorit će se ova stranica sa popisom svih dostupnih Watsonovih usluga.

Kliknite odjeljak **Speech to Text** da biste otvorili ovu stranicu s opcijama postavljanja.

Ovdje trebate samo kliknuti dugme **Create** i sa tim ste završili. Zadane vrijednosti mogu se ostaviti kakve jesu.

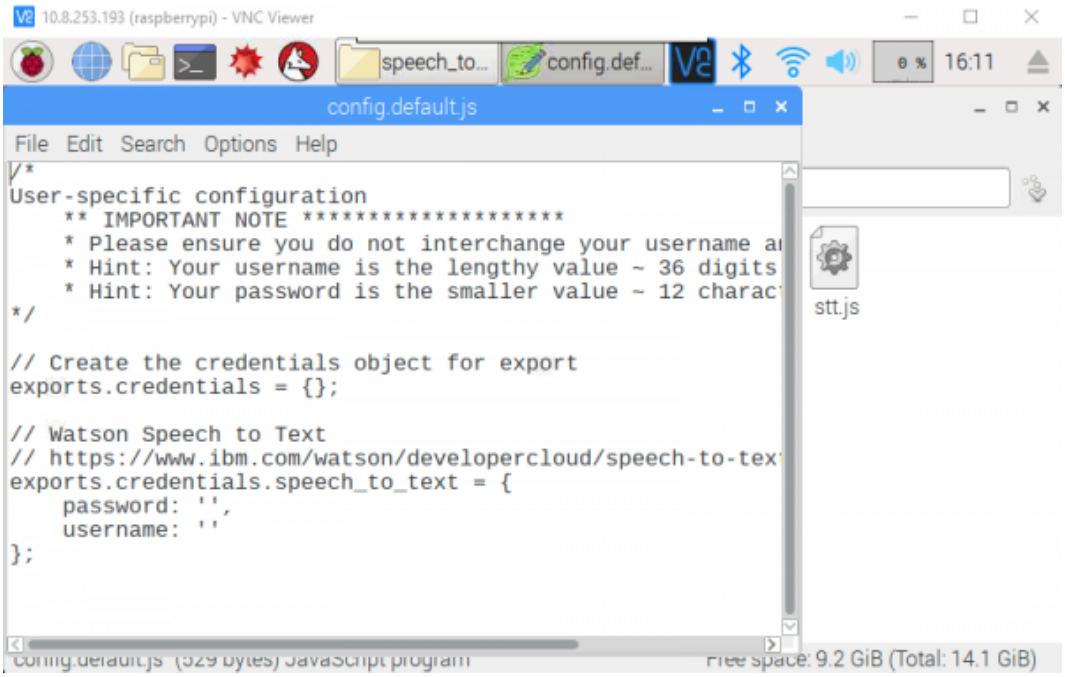
Sada ćete trebati dohvatiti (eng. fetch) **credentials** za vašu instancu **Speech to Text**, pa kliknite **Service credentials** uz lijevi rub stranice.

Ova aktivnost će vas dovesti na narednu stranicu. Da biste vidjeli svoje credentials, kliknite padajući meni **View credentials** na sredini stranice pod **ACTIONS**.

Kopirajte vjerodajnice u datoteku za konfiguraciju Raspberry Pi

Sada moramo kopirati te credentials u datoteku na Raspberry Pi. Ako do sada niste radili na Raspberry Pi, vjerojatno je najlakše biti prijavljen na Pi i otvoriti web stranicu IBM Cloud na Piovom web pregledniku.

Datoteka koju trebate izmijeniti nalazi se u **Desktop / tjbot / recipes / speech_to_text** i naziva se `config.default.js`. Dvostrukim klikom na datoteku otvorit ćete je u editoru teksta. Zatim možete copy/paste nove podatke.



Kopirajte i zalijepite **username** i **password** sa web stranice u tekstualni dokument. Imajte na umu da se redoslijed njih dviju mijenja! Na web stranici korisničko ime je iznad lozinke, ali u tekstualnom dokumentu to je lozinka iznad korisničkog imena. Nakon što unesete podatke, morate kliknuti **Save as…** dokument da biste promijenili njegovo ime. Novo ime je `config.js`.

Napomena: Credentials na stranici **IBM AI/Watson Speech-to-text** promijenjene su u API format:

```
{
  "apikey": "**XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX**",
  "iam_apikey_description": "Auto generated apikey during resource-key operation for Instance - crn:v1:bluemix:public:speech-to-text:XXXXXXX:XXXXXXXXXXXXblah-blah-blahXXXXXXXXXXXXXXXX",
  "iam_apikey_name": "auto-generated-apikey-**XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX**",
  "iam_role_crn": "XXXXXXXXXXblah-blah-blahXXXXXXXXXXX",
  "iam_serviceid_crn": "XXXXXXXXXblah-blah-blahXXXXXXXXXXX",
```

```
  "url":   "https://stream.watsonplatform.net/speech-to-text/api"
}
```

Korisničko ime (Username):

Vaše korisničko ime sadrži unos **`iam_apikey_name`**, ali samo odjeljak **`XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX`**. Izuzmite **`auto-generated-apikey-`** dio tog unosa.

```
"iam_apikey_name":      "auto-generated-apikey-XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX",
```

Lozinka (Password:

Vaša lozinka / API ključ nalazi se u unosu **`iam_apikey_name`**; ona bi trebala biti ovako strukturirana: **`XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX`**. Morat ćete izmijeniti unos datoteke **`config.js`** iz **password** u **apikey**.

```
 "apikey": "XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX",
```

Vaša datoteka **`config.js`** trebala bi imati sljedeći format:

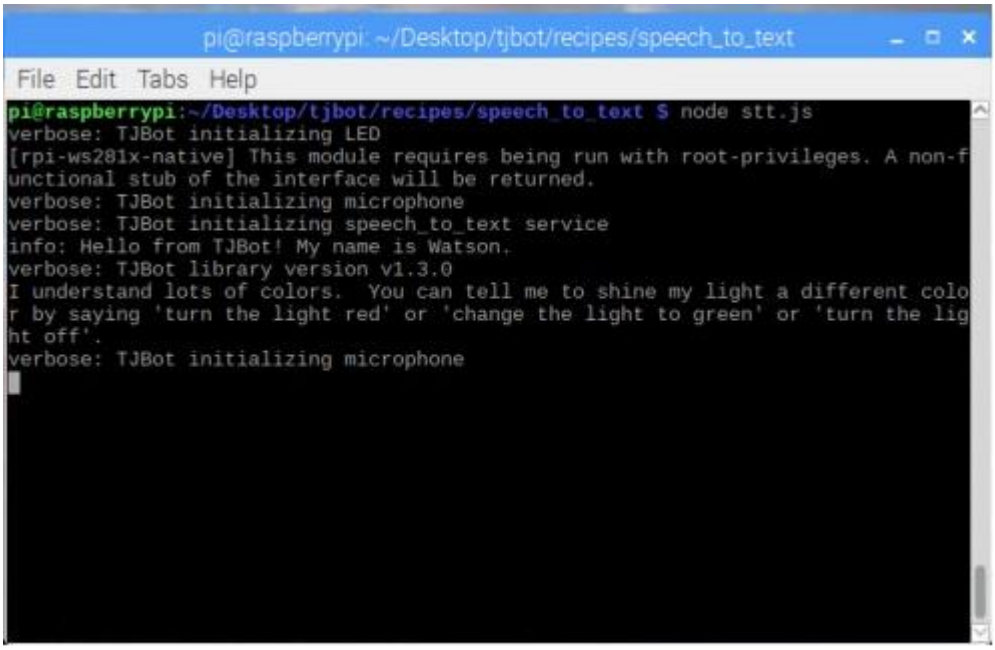
```
/*
 * User-specific configuration
 * IMPORTANT NOTES:
 *  Please ensure you do not interchange your username and password.
 *  Your username is the longer value: 36 digits, including hyphens
 *  Your password is the smaller value: 12 characters
*/
// Create the credentials object for export<br>
exports.credentials = {};
// Watson Speech to Text
// https://www.ibm.com/watson/services/speech-to-text/
exports.credentials.speech_to_text = {
    apikey: 'XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX',
    username: 'XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX'
};
```

Na dobrom ste putu. Sada je potrebno da instalirate u pokrenete uslugu pretvaranja govora u tekst

Otvorite command line u Pi i pokrenite sljedeće naredbe:

```
cd Desktop/tjbot/recipes/speech_to_text
npm install
sudo node stt.js
```

Korak **`npm install`** potrajat će neko vrijeme. Jednom kada izdate naredbu **`node stt.js,`** vidjet ćete ovo:



Sada možete izdati glasovnu naredbu TJBot-u (na engleskom jeziku) za promjenu boje LED-a, poput "**Turn the light red**", "**Turn the light blue**" ili "**Turn the light off** ".

Prilično lijepo, ha?

Isprobajte glasovne naredbe za promjenu boje LED-a.

Kad završite, pritisnite **Ctrl+C** da biste zatvorili skriptu.

Analizator sentimenta tona

Naš sljedeći projekt koristi Watsonov analizator tonova za analizu nedavnih tweetova na Twitter-u i dobivanje osjećaja za njihov ukupni emocionalni ton.

Ovaj projekat vam može pomoći da se bolje upoznate sa mogućnostima koje donosi Watson u analizi podataka pomoću analizatora tona.

Da bi pokrenuli ovu uslugu prvo trebate kreirati instancu analizatora tona.

Ponovite korake koje ste koristili kada ste kreirali nstancu **Speech to Text** s tim da sada treba da obaerete uslugu **Tone Analyzer**.

Opet, ostavite zadane vrijednosti na mjestu i pritisnite **Create**.

Nakon toga, ponovite korake korištene za preuzimanje **credentials** sa IBM Cloud i stavite ih u datoteku na Raspberry Pi.

Ovaj put ćete datoteku `config.default.js` pronaći u `Desktop/tjbot/receipts/sentiment_analysis`".

Međutim, nemojte ga zatvoriti kad završite s ovim korakom.

Za ovaj zadatak potrebno je da kreirate Twitter App za pristup nedavnim tweetovima

Za ovaj korak trebat će vam Twitter račun, pa idite na Twitter i prijavite se ako ga već nemate.

Kliknite na dugme **Create an app** da biste se preusmjerili na narednu stranicu na IBM Cloud. Ispunite prazna mjesta po vašem izboru (imajte na umu da naziv aplikacije mora biti jedinstven, tako da ne možete ponovno upotrijebiti "TJBot"), potvrdite okvir, a zatim kliknite dugne **Create your Twitter application**.

Tada će vam se pojaviti stranica s pojedinostima iz postupka kreiranja aplikacije.

Odmah ispod naziva vaše aplikacije (velikim podebljanim slovima na vrhu stranice) vidjet ćete karticu pod nazivom **Keys and Access Tokens**. Kliknite na ovo da biste otvorili narednu stranicu.

Sada trebate uzeti nekoliko podataka s ove stranice koje trebate zaliijepiti u konfiguracijsku datoteku koju ste predhdno otvorili.

Kao što možete vidjeti u nastavku, postoje četiri informacije vezane uz Twitter koje treate prikupiti. Započet ćemo sa `consumer_key` i `consumer_secret`. Oboje imaju isto ime na web stranici kao i u datoteci konfiguracije; kopirajte ih i zalijepite s web tranice u konfiguracijsku datoteku.

```
*config.default.js
File  Edit  Search  Options  Help
exports.sentiment_analysis_frequency_sec = 30; // analyze

// Create the credentials object for export
exports.credentials = {};

// Watson Tone Analyzer
// https://www.ibm.com/watson/developercloud/tone-analyzer
exports.credentials.tone_analyzer = {
    password: '[redacted]',
    username: '[redacted]'
};

// Twitter
exports.credentials.twitter = {
    consumer_key: '',
    consumer_secret: '',
    access_token_key: '',
    access_token_secret: ''
};
```

DSada trebate da popunite polja **`access_token_key`** I **`access_token_secret`**. Da biste to učinili, pomaknite se prema dolje na web stranici dok ne vidite dugme **Create my access token**.

Kliknite ga i dobit ćete novi prikaz.:

Kopirajte i zalijepite **`access_token_key`** i **`access_token_secret`** u konfiguracijsku datoteku. Zatim kliknite **Save as…** i dajte joj ime "**config.js**".

Spremni ste za sljedeći korak!

A to je da pokrenete aplikaciju.

Tako jedino možete provjeriti vaš recept na djelu! Kao i prije, otvorite prozor terminala na Raspberry Pi i upišite ove naredbe:

```
cd Desktop/tjbot/recipes/sentiment_analysis

npm install

node sentiment.js
```

Zapamtite, za korak **`npm_install`** treba neko vrijeme, pa budite strpljivi. Nakon što pokrenete korak **`node_sentiment.js`**, trebali biste imati zaslon koji izgleda ovako:

```
pi@raspberrypi: ~/Desktop/tjbot/recipes/sentiment_analysis
File  Edit  Tabs  Help
pi@raspberrypi:~/Desktop/tjbot/recipes/sentiment_analysis $ node sentiment.js
verbose: TJBot initializing LED
[rpi-ws281x-native] This module requires being run with root-privileges. A non-f
unctional stub of the interface will be returned.
verbose: TJBot initializing tone_analyzer service
info: Hello from TJBot! My name is Watson.
verbose: TJBot library version v1.3.0
I am monitoring twitter for education. It may take a few moments to collect enou
gh tweets to analyze.
verbose: TJBot shining my LED to RGB color #000000
Performing sentiment analysis of the tweets
Analyzing tone of 46 tweets
Current emotion around education is joy
verbose: TJBot shining my LED to RGB color #FFFF00
```

Trebat će nekoliko trenutaka da aplikacija skupi dovoljno tweetova (najmanje 100) da bi mogla pokrenuti analizator tonova, ali kad se dogodi, ispisat će redak s trenutnom emocijom koja okružuje ključnu riječ koju traži, kao i promjena boje LED-a.

Kad završite, samo pritisnite **Ctrl+c** da biste zatvorili skriptu.

Razgovarajte s TJBotom

Došli smo do naše posljednje vježbe.

Iskreno vam čestitamo.

Za sami kraj ostavili smo jednu od najnaprednijih usluga koje možete kreirati zahvaljujući naprednim kognitivnim sposobnostima IBM Watson.

U ovo vježbi ćemo istražiti kreiranje usluge razgovra I pretvaranja tekstaa u govor kako bi TJBot barem minimalno mogao razgovarati sa vama.

Prvi korak ka tome jeste da spojite zvučnik na Raspberry Pi.

Kao i kod napajanja, na samo jedno mjesto može se spojiti zvučnik. Ako odlučite, možete spojiti kabel za punjenje zvučnika na USB priključak na Raspberry Pi kako biste osigurali da zvučnik radi i ostaje potpuno napunjen.

Da bi omogućili uslugu razgovora potrebno je da kreirate novu **Watson Services.**

Kao i u posljednja dva recepta, trebate kreirati instancu usluga **Conversation** i **Text to Speech**. Također će biti potrebno da upotrijebite uslugu **Speech to Text** koju ste kreirali

za prvi recept. Morat ćete dohvatiti *credentials* za te usluge i staviti ih, pogađate, u konfiguracijsku datoteku na Raspberry Pi.

Ovaj put ćete datoteku `config.default.js` pronaći pod `Desktop/tjbot/receipts/conversation`.

Otvorite ga u editoru teksta.

Započnite s uslugom **Speech to text**.

Možete se vratiti na svoju nadzornu ploču i kliknuti na naziv usluge da biste otvorili poznatu stranicu **Service credentials** na lijevom rubu ili možete kopirati vjerodajnice iz konfiguracijske datoteke stvorene za prvi recept.

Nakon što to uradite potrebno je da kreirate instance **Speech to text**, slijedeći istu metodu koju ste koristili za stvaranje instanci u prva dva recepta. Još jednom možete ostaviti zadane vrijednosti na mjestu i samo pritisnuti **Create**.

Kopirajte vjerodajnice u tekstualni dokument.

Na kraju, stvorite instance **Conversation**.

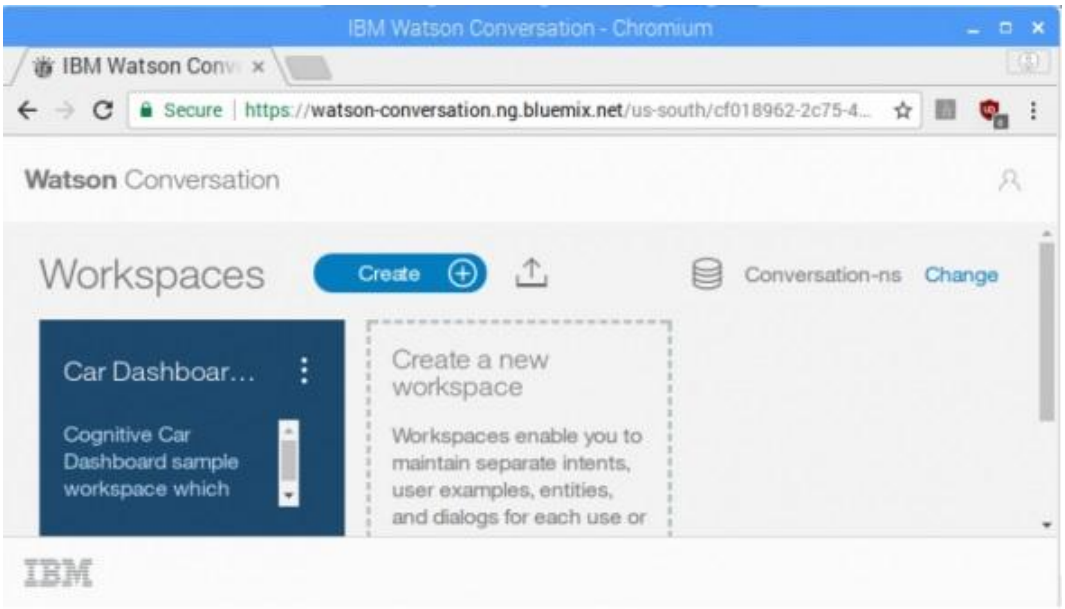
Ovaj zadatak je malo kompliciraniji.

Za prvi dio radi isto kao i tri druge usluge koje smo stvorili, pa samo slijedite te korake i kopirajte vjerodajnice u tekstualni dokument.

Zadane postavke ponovno će biti dovoljne.

Posljednji važan podatak koji nam treba je ID radnog prostora za razgovor to jest **Conversation workspace ID**. Pronađite prazno mjesto za to pri vrhu tekstualne datoteke, odmah iznad područja credentials za uslugu Watson **Conversation**. Da biste to stekli, idite na IBM Watson Conversation website (trenutno: https://assistant-us-south.watsonplatform.net/login) i prijavite se s istim ID-om koji ste koristili IBM Cloud. Obavezno to učinite na **Pi web-browseru**.

Nakon prijave, vidjet ćete ovu stranicu:

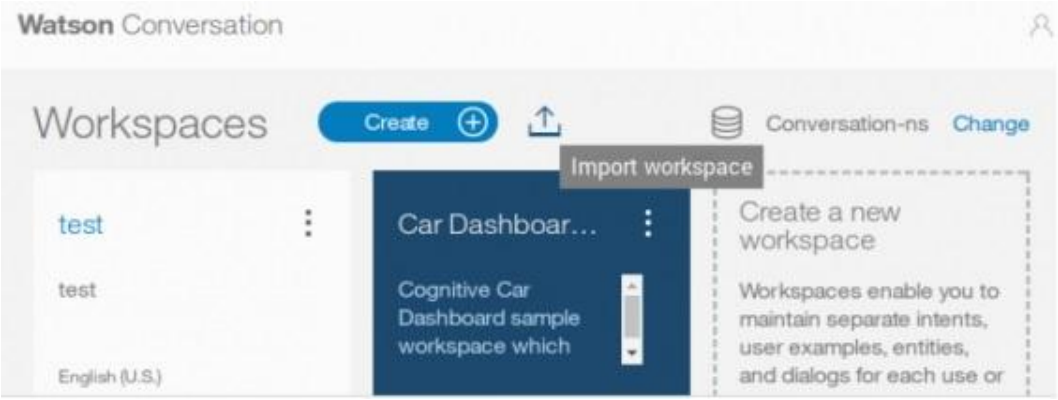


Sada trebate upload datoteku, ali prvo, trebate stvoriti novi **workspace**.

Kliknite dugme **Create**, zatim dodijelite naziv svom radnom prostoru (nije važno kako ćete ga nazvati) i opet kliknite dugme **Create**.

To će vas odvesti na narednu stranicu. Kliknite **Watson Conversation** na vrhu stranice za povratak na glavnu stranicu **Watson Conversation Workspace**.

Sa ovim korakom vi ćete se vratiti na glavnu stranicu. Kliknite malo dugme **Upload** (polučetverougao sa strelicom prema gore) pored dugmeta **Create**. Ako zadržite pokazivač miša iznad gumba, pojavit će se tekstualni okvir s riječima **import workspace** kao što je prikazano dole.

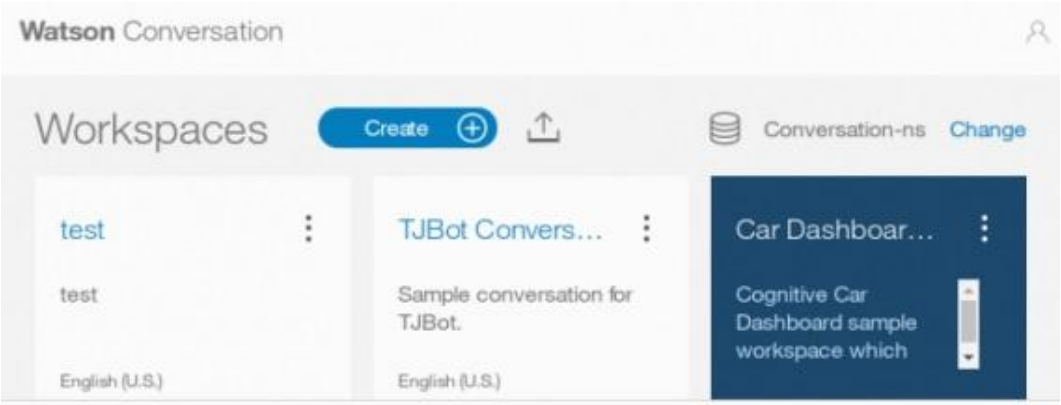


Klikom na to dugme otvorit će se novi prozor. Kliknite okvir **Choose a file** i pronađite datoteku

`Desktop/tjbot/receipt/conversation/workspace-sample.json`.

Ostavite istaknuti radio dugme **Everything**, a zatim kliknite **Import**. To će vas odvesti na narednu stranicu.

Na toj stranici kliknite **Watson Conversation** na vrhu stranice za povratak na glavnu stranicu **Watson Conversation Workspace**.



Kliknite tri vertikalno poravnate tačke u okviru **TJBot Conversation** i odaberite **View Details**. Sadržaj okvira će se promijeniti; pomaknite se prema doljeu okviru i pronađite **Workspace ID**, što je posljednji podatak koji nam je potreban da bi ovaj recept radio! Kopirajte ga s ove web stranice u tekstualni document i **Save as…** dokument na ime `config.js` i zatvorite ga.

Sada vam ostaje zadnji korak da pokrenite aplikaciju.

Ovaj bi dio trebao izgledati vrlo poznato. Otvorite prozor terminala na Raspberry Pi i unesite ove tri naredbe:

```
cd Desktop/tjbot/recipes/conversation
npm install
node conversation.js
```

Opet, pričekajte da se dovrši `npm install`.

Nakon što unesete naredbu `node conversation.js`, na terminalu vidićete instrukciju kako započeti konverzaciju sa TJBot. Na primjer možete reći: “**Watson, tell me a joke!”** ili "**Watson, who are you?**" Vi možete eksperimentisati s različitim načinima traženja (na primjer, "Watson, čujmo šalu" djeluje jednako dobro kao i "Watson, reci mi vic"). Istražite moć obrade jezika koju Watson može učiniti.

Kada završite, pritisnite **Ctrl+c** da biste zatvorili skriptu.

Sad kad ste uspješno pokrenuli svoj TJBot, vrijeme je da ga uključite u svoj projekt!

Za više informacija možete pogledati resurse koji stoje na raspolaganju u GitHub repozitoriju za TJBot I TJBot Receipts.

Priručnik **Projekt menadžment** kreiran sa ciljem da vas na sveobuhvatan način upozna sa procesom, alatima I tehnikama koji se koriste prilikom razvoja organizacijske strategije, konceptima primjene poslovne analitike u poslovanju, te da vas upozna sa sveobuhvatnim pristupom razvoja i upravljanje projektima.

Priručnik sadrži niz savremenih i širokokorištenih alata i tehnika koje se primljenjuju u kompanijama I organizacijama iz različitih industrija, zbog čega vam on može pomoći da unaprijedite svoja znanja i vještine iz poslovne administracije i projektnog menadžmenta bez obzira čime se vaša kompanija / organizacija trenutno bavi.

Priručnik je kreiran kako bi vam pomogao da savladate nastavno gradivo ALDI trening programom za Projektni menadžment (AITI.PRM.300).

Nadamo se da smo u tome uspjeli.