Internet stvari – primeri primene i bezbednost IoT sistema

Aleksandar Peulić

Uvod

U ovom predavanju nastavljamo sa osnovama Internet stvari koje smo započeli prošle nedelje. U prethodnom predavanju govorili smo o definiciji IoT, arhitekturi sistema, komunikacionim tehnologijama, kao i o senzorima i aktuatorima.

U ovom predavanju fokusiraćemo se na dva veoma važna aspekta IoT sistema. Prvi deo predavanja posvećen je primerima primene IoT tehnologije u različitim oblastima, kao što su pametne kuće, pametni gradovi, industrija i zdravstvo. Drugi deo predavanja bavi se bezbednošću IoT sistema, što danas predstavlja jedan od najvećih izazova u ovoj oblasti.

Posebna pažnja biće posvećena bezbednosti na nivou hardvera, bezbednosti na nivou edge uređaja i bezbednosti komunikacije u IoT mrežama. Cilj predavanja je da studenti razumeju kako IoT sistemi funkcionišu u realnim aplikacijama i koji su najveći bezbednosni izazovi prilikom njihove implementacije.

Plan predavanja

Na početku ćemo kratko ponoviti osnovnu arhitekturu IoT sistema, kako bismo imali jasnu sliku o tome gde se nalaze pojedini elementi bezbednosti. Nakon toga prelazimo na konkretne primene IoT tehnologije.

Posebno ćemo razmotriti četiri važne oblasti u kojima se IoT danas najviše koristi. Prva oblast su Smart Home sistemi, odnosno pametne kuće, gde IoT uređaji omogućavaju automatizaciju rasvete, grejanja, sigurnosnih sistema i drugih funkcija u domu. Druga oblast su Smart City sistemi, gde se IoT koristi za upravljanje gradskom infrastrukturom, na primer za pametni parking, monitoring kvaliteta vazduha i upravljanje saobraćajem. Treća oblast je Industrial IoT, odnosno primena IoT tehnologije u industriji i proizvodnji, gde senzori prate stanje mašina i omogućavaju prediktivno održavanje. Četvrta oblast je IoT u zdravstvu, gde IoT uređaji omogućavaju kontinuirano praćenje zdravstvenih parametara pacijenata.

U drugom delu predavanja govorićemo o bezbednosti IoT sistema, što je izuzetno važna tema jer su IoT uređaji često povezani sa kritičnim sistemima i osetljivim podacima. Posebno ćemo analizirati bezbednost na nivou hardvera i edge uređaja, jer upravo tu počinje sigurnost svakog IoT sistema.

Osnovna arhitektura IoT sistema

Pre nego što počnemo sa primerima primene IoT sistema, važno je da još jednom pogledamo osnovnu arhitekturu IoT sistema. Tipičan IoT sistem sastoji se od nekoliko ključnih slojeva.

Prvi sloj čine senzori. Senzori prikupljaju podatke iz fizičkog sveta, kao što su temperatura, vlaga, pritisak, pokret, osvetljenje ili položaj. Ti podaci se zatim šalju ka edge uređaju, odnosno IoT čvoru. To je obično mikrokontroler ili mali računar, na primer ESP32, STM32 ili Raspberry Pi.

Edge uređaj ima nekoliko važnih funkcija: prikuplja podatke sa senzora, vrši osnovnu obradu i priprema podatke za slanje preko mreže. Nakon toga podaci se šalju ka gateway uređaju. Gateway služi kao posrednik između lokalne mreže senzora i interneta. Gateway zatim prosleđuje podatke ka cloud platformi.

U cloud-u se vrši skladištenje podataka, analiza podataka, pokretanje algoritama i integracija sa drugim sistemima. Na kraju, korisnici pristupaju tim podacima kroz različite aplikacije, kao što su web dashboard, mobilna aplikacija ili industrijski SCADA sistem.

Ovakva arhitektura predstavlja osnovu gotovo svih IoT sistema koje ćemo videti u nastavku predavanja.

Najvažnije oblasti primene IoT tehnologije

Internet stvari danas predstavljaju jednu od najbrže rastućih oblasti informacionih tehnologija. IoT sistemi primenjuju se u velikom broju različitih sektora, od svakodnevnih kućnih uređaja pa sve do industrijskih i infrastrukturnih sistema.

Jedna od najpoznatijih oblasti primene jeste Smart Home, odnosno pametne kuće. U tim sistemima IoT uređaji omogućavaju automatsko upravljanje rasvetom, grejanjem, sigurnosnim sistemima i drugim uređajima u domu.

Druga veoma važna oblast su Smart City sistemi, gde se IoT koristi za upravljanje infrastrukturom gradova. Primeri uključuju pametni parking, senzore kvaliteta vazduha, pametnu rasvetu i monitoring saobraćaja.

Treća oblast je Industrial IoT, odnosno primena IoT tehnologije u industriji. U industriji se IoT koristi za nadzor mašina, optimizaciju proizvodnje i prediktivno održavanje opreme.

IoT takođe ima veoma važnu ulogu u zdravstvu, gde se koristi za daljinsko praćenje pacijenata i nosive medicinske uređaje.

Pored toga, IoT se koristi i u pametnoj poljoprivredi, transportu i logistici, kao i u energetskim sistemima. U nastavku predavanja detaljnije ćemo analizirati nekoliko najvažnijih primera IoT sistema.

Smart Home – IoT u pametnim kućama

Jedna od najrasprostranjenijih primena Internet stvari danas jeste Smart Home, odnosno koncept pametne kuće. U pametnoj kući različiti uređaji povezani su na internet i mogu međusobno da komuniciraju.

Primeri IoT uređaja u pametnoj kući su pametni termostati koji automatski regulišu temperaturu u kući, pametna rasveta koja se može kontrolisati putem mobilne aplikacije, sigurnosne kamere koje omogućavaju daljinski video nadzor, pametne brave koje omogućavaju otključavanje vrata putem telefona, kao i senzori pokreta koji detektuju prisustvo osoba.

Ovi uređaji povezani su preko kućne mreže, najčešće koristeći WiFi, ZigBee ili Bluetooth komunikaciju.

Prednosti pametnih kuća su brojne. Prva prednost je automatizacija. Uređaji mogu automatski reagovati na određene događaje. Na primer, svetlo se može uključiti kada senzor detektuje pokret. Druga prednost je energetska efikasnost, jer pametni sistemi mogu optimizovati potrošnju energije u domu. Treća prednost je daljinsko upravljanje, pošto korisnik može kontrolisati uređaje putem mobilne aplikacije sa bilo koje lokacije. Četvrta prednost je povećana bezbednost, jer sigurnosni sistemi mogu automatski detektovati neovlašćeni pristup i poslati upozorenje vlasniku.

Arhitektura Smart Home sistema

Da bismo razumeli kako funkcioniše pametna kuća, potrebno je pogledati arhitekturu sistema. Na prvom nivou nalaze se senzori i uređaji. To mogu biti senzori temperature, senzori pokreta, senzori otvaranja vrata ili pametni prekidači za rasvetu.

Ovi senzori povezani su sa IoT uređajem, koji obično predstavlja mikrokontroler, kao što su ESP32, STM32 ili Raspberry Pi. Taj uređaj prikuplja podatke sa senzora i šalje ih preko mreže. Komunikacija se najčešće ostvaruje putem kućnog WiFi rutera.

Podaci se zatim šalju ka cloud platformi, gde se vrši njihovo skladištenje i analiza. U cloud platformi mogu se pokretati različiti algoritmi koji analiziraju podatke i donose odluke. Na primer, sistem može automatski uključiti grejanje ako temperatura padne ispod određene vrednosti.

Korisnik zatim pristupa tim podacima putem mobilne aplikacije, gde može da vidi stanje sistema, primi obaveštenja ili upravlja uređajima u kući. Ovakva arhitektura koristi se u većini komercijalnih Smart Home sistema.

Smart City – IoT u pametnim gradovima

Jedna od najvažnijih oblasti primene Internet stvari danas jeste koncept pametnih gradova, odnosno Smart City. Cilj pametnih gradova je da se korišćenjem senzora i digitalnih tehnologija poboljša upravljanje gradskom infrastrukturom.

IoT senzori mogu se postaviti na različitim mestima u gradu kako bi prikupljali podatke o različitim parametrima. Jedan od najpoznatijih primera jeste pametni parking sistem. U takvom sistemu senzori detektuju da li je parking mesto slobodno ili zauzeto. Te informacije zatim se šalju u centralni sistem koji vozačima može pokazati gde postoje slobodna parking mesta.

Drugi veoma važan primer jeste monitoring kvaliteta vazduha. U gradovima se mogu postaviti senzori koji kontinuirano mere koncentraciju zagađujućih čestica i gasova, kao što su PM2.5, PM10, CO_2 i NO_2.

IoT tehnologija koristi se i za pametnu rasvetu. U takvim sistemima rasveta se automatski prilagođava u zavisnosti od prisustva ljudi ili nivoa osvetljenja. Pored toga, IoT sistemi mogu pomoći u upravljanju saobraćajem analizom protoka vozila i optimizacijom rada semafora.

Osnovni ciljevi Smart City sistema su smanjenje troškova infrastrukture, povećanje energetske efikasnosti i poboljšanje kvaliteta života građana.

LoRaWAN u Smart City sistemima

U Smart City sistemima često se koristi LoRaWAN tehnologija, koja je posebno dizajnirana za IoT uređaje. LoRaWAN omogućava komunikaciju na velikim udaljenostima uz veoma malu potrošnju energije.

U tipičnom Smart City sistemu senzori su raspoređeni po gradu. To mogu biti senzori koji mere kvalitet vazduha, nivo buke, temperaturu ili zauzetost parking mesta. Ti senzori šalju male pakete podataka preko LoRa radio komunikacije.

Podaci se zatim primaju na LoRaWAN gateway uređaju. Gateway predstavlja uređaj koji povezuje LoRa mrežu sa internetom. Gateway zatim prosleđuje podatke ka Network Serveru, koji upravlja mrežom i identifikacijom uređaja. Nakon toga podaci se šalju na cloud platformu, gde se vrši skladištenje i analiza podataka.

Na kraju, korisnici mogu pristupiti tim podacima preko dashboard aplikacija koje vizualizuju podatke u realnom vremenu. Ovakvi sistemi omogućavaju gradovima da bolje prate stanje infrastrukture i donose kvalitetnije odluke na osnovu podataka.

Industrial IoT – Industrija 4.0

Jedna od najvažnijih oblasti primene IoT tehnologije danas jeste Industrial IoT, koji je deo koncepta Industrija 4.0. Industrija 4.0 predstavlja novu fazu industrijske revolucije u kojoj se digitalne tehnologije koriste za unapređenje proizvodnih procesa.

U industrijskim sistemima IoT senzori se postavljaju na mašine kako bi se kontinuirano pratili različiti parametri rada. Na primer, mogu se meriti vibracije mašine, temperatura motora, potrošnja energije i brzina rotacije.

Ovi podaci zatim se analiziraju kako bi se otkrili potencijalni problemi pre nego što dođe do kvara. Ovaj pristup naziva se prediktivno održavanje. Prediktivno održavanje omogućava da se kvarovi predvide unapred, čime se smanjuju troškovi i izbegavaju prekidi proizvodnje.

Pored toga, IoT sistemi mogu pomoći u optimizaciji proizvodnje, jer omogućavaju detaljan uvid u rad proizvodnih linija. U ovim sistemima često se koriste edge computing uređaji, koji vrše lokalnu obradu podataka blizu mašina. To omogućava bržu reakciju sistema i smanjuje potrebu za slanjem velikih količina podataka u cloud.

IoT u zdravstvu

Internet stvari imaju veoma važnu primenu u oblasti zdravstva, gde omogućavaju razvoj takozvanog Internet of Medical Things, odnosno mreže medicinskih uređaja povezanih na internet.

Jedan od najpoznatijih primera su nosivi uređaji, odnosno wearable uređaji. To su uređaji kao što su pametni satovi, fitness narukvice i medicinski senzori. Ovi uređaji mogu kontinuirano pratiti različite zdravstvene parametre, na primer srčani ritam, nivo kiseonika u krvi, broj koraka i kvalitet sna.

Prikupljeni podaci mogu se automatski slati lekarima ili zdravstvenim sistemima na analizu. Ovakav pristup omogućava daljinski monitoring pacijenata, što je posebno važno za osobe sa hroničnim bolestima.

IoT tehnologija takođe omogućava razvoj telemedicine, gde pacijenti mogu komunicirati sa lekarima na daljinu uz korišćenje digitalnih uređaja. U modernim zdravstvenim ustanovama razvijaju se i pametne bolnice, gde IoT sistemi prate medicinsku opremu, pacijente i uslove u bolnici.

Ovakvi sistemi mogu značajno unaprediti kvalitet zdravstvene zaštite i smanjiti troškove zdravstvenog sistema.

Bezbednost – najveći izazov IoT sistema

Iako IoT sistemi donose mnoge prednosti, oni takođe predstavljaju veliki bezbednosni izazov. Jedan od osnovnih problema jeste ogroman broj povezanih uređaja. Svaki od tih uređaja može predstavljati potencijalnu tačku napada.

Drugi problem je što IoT uređaji često imaju ograničene hardverske resurse. Mnogi uređaji koriste male mikrokontrolere koji imaju ograničenu memoriju i procesorsku snagu, zbog čega je implementacija naprednih bezbednosnih mehanizama otežana.

Treći problem jeste slaba autentifikacija. Mnogi IoT uređaji koriste podrazumevane lozinke ili uopšte nemaju adekvatnu zaštitu pristupa. Takođe, mnogi IoT uređaji se retko ažuriraju, što znači da poznate bezbednosne ranjivosti često ostaju neispravljene.

Ako napadač uspe da kompromituje IoT uređaj, posledice mogu biti ozbiljne. Napadač može ukrasti podatke, preuzeti kontrolu nad uređajem ili koristiti uređaj kao deo botnet mreže za izvođenje napada na druge sisteme.

Šta je botnet?

Botnet je mreža povezanih uređaja, kao što su računari i IoT uređaji, koji su zaraženi zlonamernim softverom i koje napadač kontroliše daljinski, bez znanja vlasnika. Takvi uređaji često se nazivaju zombiji. Oni primaju komande sa centralnog komandno-kontrolnog servera kojim upravlja napadač.

Botneti se najčešće koriste za DDoS napade, odnosno preplavljivanje veb sajtova i servera ogromnim brojem zahteva kako bi prestali da rade. Pored toga, mogu se koristiti za krađu podataka, kao što su lozinke, podaci o platnim karticama i lični podaci, kao i za masovno slanje neželjenih mejlova.

Do infekcije uređaja može doći putem malicioznih mejlova, sumnjivih sajtova ili iskorišćavanjem ranjivosti u softveru.

Mirai botnet – poznat primer IoT napada

Jedan od najpoznatijih napada koji pokazuje koliko IoT uređaji mogu biti opasni jeste Mirai botnet napad iz 2016. godine. Mirai je bio maliciozni softver koji je napadao IoT uređaje povezane na internet.

Napadači su skenirali internet u potrazi za uređajima koji koriste podrazumevane korisničke naloge i lozinke. Mnogi IoT uređaji, kao što su sigurnosne kamere i ruteri, prodavali su se sa fabričkim lozinkama koje korisnici nikada nisu promenili.

Mirai je automatski pokušavao da se prijavi na te uređaje koristeći poznate kombinacije korisničkog imena i lozinke. Kada bi uspeo da pristupi uređaju, instalirao bi maliciozni program i pretvorio uređaj u deo botnet mreže.

Napadači su zatim koristili hiljade ovih uređaja za izvođenje DDoS napada, odnosno napada koji preopterećuju servere ogromnim brojem zahteva. U jednom od najvećih napada Mirai botnet je generisao ogroman saobraćaj koji je doveo do pada velikih internet servisa kao što su Twitter, Netflix, GitHub i Reddit.

Ovaj napad pokazao je da čak i mali IoT uređaji mogu predstavljati ozbiljnu bezbednosnu pretnju kada se koriste u velikom broju.

Slojevi bezbednosti u IoT sistemima

Bezbednost IoT sistema ne može se rešiti samo na jednom mestu u sistemu. IoT sistemi su složeni i sastoje se od više različitih komponenti, zbog čega bezbednost mora biti implementirana na više nivoa arhitekture sistema.

Prvi nivo je device layer, odnosno sloj uređaja. Ovaj sloj obuhvata senzore, mikrokontrolere i druge IoT uređaje koji prikupljaju podatke. Na ovom nivou veoma je važno obezbediti zaštitu firmware-a, kontrolu pristupa uređaju i sigurnu identifikaciju uređaja.

Drugi nivo je network layer, odnosno sloj komunikacije. Ovde je cilj zaštititi podatke tokom prenosa između uređaja i servera. To se postiže korišćenjem enkripcije i sigurnih komunikacionih protokola.

Treći nivo je edge ili gateway sloj. Gateway uređaji povezuju lokalne IoT mreže sa internetom i često vrše lokalnu obradu podataka. Ovi uređaji moraju biti zaštićeni jer predstavljaju ključnu tačku sistema.

Četvrti nivo je cloud sloj, gde se podaci skladište i analiziraju. Ovde je veoma važno obezbediti kontrolu pristupa i zaštitu baze podataka.

Poslednji nivo je application layer, odnosno sloj aplikacija koje koriste korisnici. Na ovom nivou implementiraju se mehanizmi autentifikacije korisnika i kontrole pristupa.

Hardverska bezbednost IoT uređaja

Bezbednost IoT sistema mora početi već na hardverskom nivou uređaja. Ako napadač može da kompromituje sam uređaj, onda svi ostali bezbednosni mehanizmi postaju beskorisni.

Jedan od najvažnijih mehanizama hardverske bezbednosti jeste Secure Boot. Secure Boot predstavlja proces u kome uređaj proverava digitalni potpis firmware-a pre nego što ga pokrene. Ako firmware nije validan ili nije potpisan od strane proizvođača, uređaj neće dozvoliti njegovo pokretanje. Na taj način sprečava se instalacija malicioznog softvera.

Drugi važan koncept jeste Hardware Root of Trust. To znači da uređaj poseduje sigurni hardverski element koji čuva kriptografske ključeve i identitet uređaja. Ovi ključevi koriste se za autentifikaciju uređaja u mreži.

Još jedan važan aspekt jeste enkripcija firmware-a. Firmware može biti šifrovan kako bi se sprečilo da napadač pročita ili modifikuje program koji se izvršava na uređaju.

Takođe je važno obezbediti secure storage, odnosno sigurno čuvanje kriptografskih ključeva i drugih osetljivih podataka. Mnogi moderni mikrokontroleri imaju posebne sigurnosne memorijske oblasti za čuvanje tajnih ključeva.

Edge Security u IoT sistemima

U klasičnim IoT sistemima svi podaci su se slali direktno u cloud, gde se vršila obrada i analiza. Međutim, sa povećanjem broja IoT uređaja i količine podataka pojavila se potreba za novim pristupom koji se naziva edge computing.

Edge computing podrazumeva da se deo obrade podataka vrši blizu izvora podataka, odnosno na samim IoT uređajima ili na gateway uređajima. Na primer, kamera može lokalno analizirati video signal i poslati samo relevantne informacije, umesto da šalje ceo video stream u cloud.

Ovakav pristup ima nekoliko prednosti. Prva prednost je manja latencija, jer se odluke donose lokalno bez potrebe za slanjem podataka na udaljeni server. Druga prednost je smanjenje mrežnog saobraćaja, jer se u cloud šalju samo obrađeni podaci. Treća prednost je bolja zaštita privatnosti, jer osetljivi podaci ne moraju napuštati lokalni sistem.

Međutim, edge uređaji predstavljaju i nove bezbednosne izazove. Napadač može pokušati da fizički pristupi uređaju i kompromituje sistem. Takođe je moguće da napadač pokuša da modifikuje firmware ili izvrši napad na gateway uređaje koji povezuju IoT mrežu sa internetom. Zbog toga je veoma važno implementirati bezbednosne mehanizme i na nivou edge uređaja.

Metode zaštite IoT sistema

Da bi IoT sistemi bili bezbedni, potrebno je primeniti više različitih bezbednosnih mehanizama.

Prvi i najvažniji mehanizam jeste autentifikacija uređaja. Svaki uređaj u IoT mreži mora imati jedinstveni identitet i mora biti verifikovan pre nego što dobije pristup mreži.

Drugi važan mehanizam jeste enkripcija komunikacije. Podaci koji se prenose između IoT uređaja i servera moraju biti šifrovani kako bi se sprečilo presretanje ili modifikovanje podataka.

Treći mehanizam jeste kontrola pristupa. Samo autorizovani korisnici i sistemi treba da imaju pristup IoT uređajima i podacima.

Četvrti važan aspekt jeste redovno ažuriranje firmware-a. Mnogi napadi na IoT uređaje koriste ranjivosti u starim verzijama firmware-a, zbog čega je veoma važno redovno ažuriranje softvera.

Peti mehanizam jeste monitoring sistema. Sistemi za nadzor mogu otkriti neobične aktivnosti u mreži i na vreme upozoriti administratore.

Još jedan važan pristup jeste segmentacija mreže. IoT uređaji se često stavljaju u posebne mrežne segmente kako bi se sprečilo da kompromitovanje jednog uređaja ugrozi čitav sistem.

Dodatni primer: jednostavan IoT sistem sa ESP32 ili STM32

Da bismo bolje razumeli kako IoT sistem funkcioniše u praksi, možemo pogledati jedan jednostavan primer.

Na početku sistema nalaze se senzori koji prikupljaju podatke iz okruženja, na primer senzor temperature i vlažnosti. Ovaj senzor povezan je sa mikrokontrolerom kao što su ESP32 ili STM32, koji prikuplja podatke i priprema ih za slanje preko mreže.

Mikrokontroler zatim šalje podatke preko WiFi mreže ka serveru, često koristeći protokol MQTT. MQTT je veoma popularan protokol u IoT sistemima jer omogućava efikasnu razmenu malih količina podataka.

Podaci se potom šalju na cloud platformu, gde se skladište i analiziraju. Na kraju, korisnik može pristupiti tim podacima putem web dashboard-a ili mobilne aplikacije.

Ovakvi sistemi koriste se u pametnoj poljoprivredi, monitoringu zgrada i industrijskom nadzoru.

Najčešći napadi na IoT sisteme

IoT sistemi često su meta različitih sajber napada. Jedan od najčešćih napada jeste brute force napad, gde napadač pokušava da pogodi korisničko ime i lozinku uređaja.

Drugi tip napada uključuje instalaciju malicioznog softvera na IoT uređaje. Kada se uređaj kompromituje, napadač može preuzeti kontrolu nad njim.

IoT uređaji se takođe često koriste u DDoS napadima, gde veliki broj uređaja istovremeno šalje ogromnu količinu saobraćaja ka određenom serveru.

Postoje i napadi koji uključuju presretanje komunikacije, gde napadač pokušava da pročita ili modifikuje podatke tokom prenosa.

Još jedan ozbiljan napad jeste kompromitovanje firmware-a, gde napadač menja softver koji se izvršava na uređaju. Zbog toga je bezbednost firmware-a jedan od ključnih aspekata zaštite IoT sistema.

Budućnost IoT tehnologije

Internet stvari će u narednim godinama imati još veći značaj u razvoju digitalnih tehnologija. Jedan od najvažnijih trendova jeste integracija IoT sistema sa veštačkom inteligencijom. Kombinacija IoT senzora i AI algoritama omogućava razvoj sistema koji mogu automatski analizirati podatke i donositi odluke.

Drugi važan trend jeste razvoj edge computing sistema, gde se sve veći deo obrade podataka pomera sa cloud servera ka lokalnim uređajima.

Veliku ulogu imaće i razvoj 5G mreža, koje omogućavaju bržu i pouzdaniju komunikaciju između velikog broja uređaja.

IoT tehnologija igraće ključnu ulogu u razvoju pametnih gradova, autonomnih vozila i naprednih industrijskih sistema. U narednim godinama očekuje se dalji rast broja povezanih uređaja i još snažnija integracija IoT sistema u svakodnevni život.

IoT sistem kroz pet nivoa

Da bismo bolje razumeli kako funkcionišu moderni IoT sistemi, možemo ih posmatrati kroz pet osnovnih slojeva arhitekture.

Prvi sloj je device layer, odnosno sloj uređaja. Ovde se nalaze senzori i aktuatori koji komuniciraju sa fizičkim svetom. Senzori prikupljaju podatke kao što su temperatura, vlaga, pokret ili pritisak.

Drugi sloj je edge layer. Na ovom nivou vrši se lokalna obrada podataka. Edge uređaji mogu filtrirati podatke i donositi brze odluke bez potrebe za slanjem svih podataka u cloud.

Treći sloj je gateway layer. Gateway uređaji povezuju lokalne IoT mreže sa internetom i često agregiraju podatke sa više senzora.

Četvrti sloj je cloud layer. U cloud-u se vrši skladištenje velikih količina podataka, analiza podataka i pokretanje različitih analitičkih algoritama.

Poslednji sloj je application layer, odnosno sloj aplikacija. Ovde korisnici pristupaju podacima putem web ili mobilnih aplikacija.

Ovaj model sa pet slojeva omogućava da jasno razumemo kako su IoT sistemi organizovani i gde se nalaze različite funkcije sistema.

Kada IoT nije bezbedan – realni incidenti

Iako IoT donosi mnoge prednosti, važno je razumeti da ova tehnologija može predstavljati i ozbiljan bezbednosni rizik. Postoji više poznatih incidenata koji pokazuju šta se može desiti kada IoT sistemi nisu adekvatno zaštićeni.

Jedan od najpoznatijih primera dogodio se 2015. godine, kada su bezbednosni istraživači uspeli da daljinski preuzmu kontrolu nad Jeep Cherokee automobilom. Napadači su uspeli da manipulišu različitim funkcijama vozila, uključujući kočenje i upravljanje. Ovaj incident pokazao je koliko povezani sistemi u vozilima mogu biti ranjivi ako nisu adekvatno zaštićeni.

Drugi primer dolazi iz oblasti zdravstva. U modernim bolnicama koristi se veliki broj povezanih medicinskih uređaja. Ako napadač kompromituje takav uređaj, može doći do ugrožavanja medicinskih podataka ili čak do prekida rada kritične medicinske opreme.

Treći primer odnosi se na industrijske sisteme. Industrijski IoT uređaji često su povezani sa sistemima koji upravljaju proizvodnim linijama. Napad na takve sisteme može dovesti do prekida proizvodnje ili oštećenja opreme.

Zbog toga je veoma važno da bezbednost bude uključena u dizajn IoT sistema od samog početka.

Pet pravila za dizajn bezbednog IoT sistema

Na kraju možemo izdvojiti nekoliko osnovnih principa koji su ključni za dizajn bezbednih IoT sistema.

Prvo pravilo je Security by Design. To znači da bezbednost mora biti planirana već u fazi projektovanja sistema, a ne dodata kasnije. Ako se bezbednost ne uzme u obzir od početka, sistem će gotovo sigurno imati ozbiljne ranjivosti.

Drugo pravilo je Strong Authentication. Svaki IoT uređaj mora imati jedinstveni identitet i mora biti autentifikovan pre nego što dobije pristup mreži.

Treće pravilo je Encrypted Communication. Podaci koji se prenose između uređaja, gateway-a i cloud sistema moraju biti šifrovani kako bi se sprečilo presretanje komunikacije.

Četvrto pravilo je Secure Firmware Updates. IoT uređaji moraju imati mogućnost sigurnog ažuriranja firmware-a kako bi se mogle ispraviti bezbednosne ranjivosti.

Peto pravilo je Continuous Monitoring. IoT sistemi moraju biti kontinuirano nadzirani kako bi se na vreme otkrile sumnjive aktivnosti ili pokušaji napada.

Ako se ova pravila poštuju, moguće je značajno povećati bezbednost IoT sistema.

Zaključak

Na kraju možemo zaključiti da Internet stvari predstavljaju jednu od najvažnijih tehnologija savremenog informacionog društva. IoT omogućava povezivanje velikog broja uređaja koji mogu automatski prikupljati i razmenjivati podatke.

Ova tehnologija već danas ima široku primenu u mnogim oblastima, uključujući pametne kuće, pametne gradove, industriju i zdravstvo. Korišćenjem IoT sistema moguće je unaprediti efikasnost sistema, smanjiti troškove i doneti bolje odluke na osnovu prikupljenih podataka.

Međutim, razvoj IoT tehnologije donosi i značajne izazove. Jedan od najvećih izazova jeste bezbednost sistema, jer veliki broj povezanih uređaja može predstavljati potencijalnu tačku napada. Takođe je veoma važna zaštita privatnosti korisnika, jer IoT uređaji često prikupljaju osetljive podatke. Pored toga, veliki izazov predstavlja i interoperabilnost uređaja, odnosno mogućnost da uređaji različitih proizvođača međusobno komuniciraju.

U budućnosti se očekuje da će IoT sistemi postati još rasprostranjeniji i igrati ključnu ulogu u razvoju digitalne ekonomije.