Internet stvari – primeri primene i bezbednost IoT sistema

Aleksandar Peulic

Plan predavanja

- Kratak pregled IoT arhitekture
- Primeri primene IoT sistema
- Smart Home sistemi
- Smart City sistemi
- Industrial IoT (Industrija 4.0)
- IoT u zdravstvu
- Bezbednost IoT sistema
- Bezbednost hardvera i edge uređaja

Osnovna arhitektura IoT sistema

Senzori (Sensors)

↓

Edge uređaj / IoT čvor

↓

Gateway

↓

Cloud platforma

↓

Aplikacije i korisnici

Glavne funkcije

- prikupljanje podataka
- komunikacija uređaja
- obrada podataka
- vizualizacija i upravljanje

Najvažnije oblasti primene IoT tehnologije

IoT tehnologija se danas koristi u mnogim oblastima:

- Smart Home (pametne kuće)
- Smart City (pametni gradovi)
- Industrial IoT (Industrija 4.0)
- Healthcare IoT (zdravstvo)
- Poljoprivreda (Smart Agriculture)
- Transport i logistika
- Energetski sistemi (Smart Grid)

Smart Home – IoT u pametnim kućama

Primeri uređaja u pametnim kućama:

- pametni termostat
- pametna rasveta
- sigurnosne kamere
- pametne brave
- senzori pokreta
- pametni kućni aparati

Smart Home – IoT u pametnim kućama

Prednosti

- automatizacija
- energetska efikasnost
- daljinsko upravljanje
- povećana bezbednost

Arhitektura Smart Home IoT sistema

Tipična struktura pametne kuće

Senzori i uređaji

↓

IoT uređaj / mikrokontroler

↓

Kućni router (WiFi)

↓

Cloud platforma

↓

Mobilna aplikacija

Arhitektura Smart Home IoT sistema

Primer tehnologija

- ESP32 / STM32
- WiFi / ZigBee / Bluetooth
- MQTT komunikacija
- Cloud platforme (AWS, Azure, ThingsBoard)

Smart City – IoT u pametnim gradovima

IoT omogućava efikasnije upravljanje gradskom infrastrukturom.

- Primeri primene
- pametni parking sistemi
- monitoring kvaliteta vazduha
- pametna rasveta
- upravljanje saobraćajem
- monitoring potrošnje energije
- upravljanje otpadom

Smart City – IoT u pametnim gradovima

Ciljevi Smart City sistema

- smanjenje troškova
- povećanje efikasnosti
- poboljšanje kvaliteta života građana

Smart City IoT arhitektura (LoRaWAN)

Tipična arhitektura sistema

IoT senzori u gradu

↓

LoRaWAN Gateway

↓

Network Server

↓

Cloud platforma

↓

Dashboard / aplikacije

Smart City IoT arhitektura (LoRaWAN)

Primer senzora

- senzori kvaliteta vazduha
- parking senzori
- meteorološki senzori
- senzori nivoa vode
- senzori buke

Industrial IoT (Industrija 4.0)

Industrial IoT omogućava digitalizaciju proizvodnih procesa.

Primeri primene

- monitoring rada mašina
- prediktivno održavanje
- optimizacija proizvodnje
- kontrola kvaliteta
- automatizacija procesa

Industrial IoT (Industrija 4.0)

Tehnologije koje se koriste

- senzori vibracija
- senzori temperature
- industrijski IoT gateway
- edge computing sistemi

IoT u zdravstvu (Healthcare IoT)

IoT omogućava kontinuirano praćenje zdravstvenog stanja pacijenata.

Primeri uređaja

- pametni satovi
- fitness narukvice
- senzori za praćenje srčanog ritma
- senzori za nivo kiseonika u krvi
- medicinski IoT uređaji za kućno praćenje pacijenata

IoT u zdravstvu (Healthcare IoT)

Primeri primene

- daljinski monitoring pacijenata
- telemedicina
- pametne bolnice
- praćenje hroničnih bolesti

Bezbednost – najveći izazov IoT sistema

IoT uređaji često predstavljaju bezbednosni rizik.

Razlozi

- veliki broj povezanih uređaja
- ograničeni resursi uređaja
- slaba autentifikacija
- nedovoljno ažuriranje firmware-a
- izloženost internetu

Bezbednost – najveći izazov IoT sistema

Moguće posledice

- krađa podataka
- kontrola uređaja od strane napadača
- botnet napadi
- ugrožavanje kritične infrastrukture

Mirai botnet – primer IoT napada

Mirai botnet (2016)

Jedan od najvećih napada na internet infrastrukturu.

Napad je koristio:

- IP kamere
- kućne rutere
- IoT uređaje
- DVR uređaje

Mirai botnet – primer IoT napada

Rezultat napada

- veliki DDoS napad
- oboreni veliki internet servisi
- Twitter, Netflix, GitHub, Reddit

Slojevi bezbednosti u IoT sistemima

Bezbednost IoT sistema mora biti implementirana na više nivoa.

Glavni slojevi bezbednosti

- Device layer (uređaji i senzori)
- Network layer (komunikacija)
- Edge / Gateway layer
- Cloud layer
- Application layer

Slojevi bezbednosti u IoT sistemima

Cilj

- zaštita uređaja
- zaštita komunikacije
- zaštita podataka

Hardware Security u IoT uređajima

Bezbednost IoT sistema počinje na nivou hardvera.

Najvažniji mehanizmi

- Secure Boot
- Hardware Root of Trust
- Enkripcija firmware-a
- Secure storage (čuvanje ključeva)
- Zaštita memorije

Hardware Security u IoT uređajima

Cilj

- sprečiti neovlašćeno pokretanje firmware-a
- zaštititi identitet uređaja
- zaštititi kriptografske ključeve

Edge Security u IoT sistemima

Edge uređaji obrađuju podatke blizu izvora podataka.

Prednosti edge obrade

- manja latencija
- manja količina podataka u mreži
- brža reakcija sistema
- bolja zaštita privatnosti

Edge Security u IoT sistemima

Bezbednosni izazovi

- fizički pristup uređaju
- kompromitovanje firmware-a
- napadi na gateway uređaje

Metode zaštite IoT sistema

Najvažniji bezbednosni mehanizmi u IoT sistemima:

- autentifikacija uređaja
- enkripcija komunikacije
- kontrola pristupa
- ažuriranje firmware-a
- monitoring sistema
- segmentacija mreže

Bezbednost

Internet stvari predstavljaju jednu od ključnih tehnologija savremenog digitalnog društva.

IoT omogućava

- automatizaciju sistema
- prikupljanje velikih količina podataka
- razvoj pametnih gradova i industrije 4.0
- napredne zdravstvene sisteme

Bezbednost

Najveći izazovi

- bezbednost sistema
- zaštita privatnosti
- interoperabilnost uređaja
- standardizacija tehnologija

Budućnost IoT tehnologije

Razvoj IoT tehnologije ide u nekoliko pravaca:

- integracija sa veštačkom inteligencijom
- razvoj edge computing sistema
- razvoj 5G mreža
- pametni gradovi i autonomni sistemi
- industrija 4.0

Budućnost IoT tehnologije

Očekivanja

Do 2030 godine očekuje se više desetina milijardi IoT uređaja.

IoT sistem kroz 5 nivoa

1. Device Layer

- senzori
- aktuatori
- mikrokontroleri

IoT sistem kroz 5 nivoa

2. Edge Layer

- lokalna obrada podataka
- filtriranje podataka
- brza reakcija sistema

IoT sistem kroz 5 nivoa

3. Gateway Layer

- povezivanje IoT mreže sa internetom
- agregacija podataka

IoT sistem kroz 5 nivoa

4. Cloud Layer

- skladištenje podataka
- analiza podataka
- IoT platforme

IoT sistem kroz 5 nivoa

5. Application Layer

- web aplikacije
- mobilne aplikacije
- dashboard sistemi

Kada IoT nije bezbedan – realni incidenti

Primeri iz realnog sveta

Hakovani automobil (2015)

Daljinski preuzeli kontrolu nad Jeep Cherokee vozilom nasred autoputa, dok je čovek koji ga je vozio bio nemoćan da se bori protiv napada!

Napadi na bolnice

IoT medicinski uređaji mogu biti meta sajber napada.

Industrijski sistemi

Napadi na industrijske kontrolne sisteme mogu zaustaviti proizvod

5 pravila za dizajn bezbednog IoT sistema

1. Security by Design

Bezbednost mora biti planirana od početka razvoja sistema.

2. Strong Authentication

Svaki uređaj mora imati jedinstveni identitet i sigurnu autentifikaciju.

3. Encrypted Communication

Svi podaci moraju biti šifrovani tokom prenosa.

4. Secure Firmware Updates

Uređaji moraju omogućiti sigurna ažuriranja firmware-a.

5. Continuous Monitoring

IoT sistemi moraju biti kontinuirano nadzirani.

Zaključak

Bezbednost mora biti ključni deo dizajna IoT sistema.