Internet věcí (IoT)

Internet věcí (IoT) je síť fyzických objektů („věcí“), které jsou vybaveny senzory, softwarem a dalšími technologiemi za účelem propojování a výměny dat s jinými zařízeními a systémy přes internet. Tato zařízení sahají od běžných domácích spotřebičů až po sofistikované průmyslové nástroje.

1. Architektura IoT systému

Fungování IoT lze rozdělit do čtyř základních vrstev:

- **Zařízení a senzory (Perception Layer):** Fyzické objekty, které sbírají data z okolí (teplota, pohyb, vlhkost, GPS souřadnice).
- **Konektivita (Network Layer):** Způsob, jakým se data přenášejí (Wi-Fi, Bluetooth, 5G, LoRaWAN, Zigbee).
- **Zpracování dat (Middleware Layer):** Analýza přijatých dat v cloudu nebo na okraji sítě (Edge Computing).
- **Aplikace (Application Layer):** Koncové rozhraní pro uživatele (mobilní aplikace, ovládací panel průmyslové linky).

---

2. Oblasti využití

IoT transformuje téměř všechna odvětví:

Chytrá domácnost (Smart Home)

Umožňuje automatizaci a vzdálené ovládání osvětlení, vytápění nebo zabezpečení.

- **Příklad:** Termostat, který se naučí váš rozvrh a upraví teplotu před vaším příchodem.

Průmyslové IoT (IIoT / Průmysl 4.0)

Využití senzorů v továrnách pro prediktivní údržbu a optimalizaci výroby.

- **Příklad:** Stroj sám nahlásí blížící se opotřebení ložiska dříve, než dojde k poruše a zastavení linky.

Chytrá města (Smart Cities)

Zlepšení kvality života a efektivity služeb ve městech.

- **Příklad:** Chytré osvětlení, které se ztlumí, když v ulici nikdo není, nebo senzory v popelnicích informující o jejich naplnění.

Elektronické zdravotnictví (eHealth)

Sledování zdravotního stavu pacientů v reálném čase mimo nemocnici.

- **Příklad:** Kardiostimulátory nebo náramky pro diabetiky, které automaticky odesílají data lékaři.

—

3. Technologie konektivity

Výběr přenosové technologie závisí na dosahu a spotřebě energie:

Technologie	Dosah	Spotřeba	Typické využití
Bluetooth / BLE	Krátký	Velmi nízká	Wearables (hodinky), fitness tagy.
Wi-Fi	Střední	Střední	Domácí spotřebiče, kamery.
5G	Velký	Vyšší	Autonomní vozidla, kritická infrastruktura.
LoRaWAN / Sigfox	Extrémní (km)	Minimální	Zemědělství, senzory v terénu (baterie vydrží roky).

—

4. Bezpečnostní výzvy IoT

Bezpečnost je největší slabinou IoT. Miliardy levných zařízení často postrádají základní ochranné prvky:

- **Slabá hesla:** Mnoho zařízení má z výroby nastavená univerzální hesla (např. „admin“), která uživatelé nemění.
- **Absence aktualizací:** Levná zařízení často nedostávají bezpečnostní záplaty.
- **Ochrana soukromí:** Neustálý sběr dat o pohybu a zvycích uživatelů v jejich domovech.
- **Botnety:** Hackeři mohou ovládnout miliony IoT zařízení a použít je k masivním DDoS útokům.

—

5. Budoucnost: AIoT

Trendem je spojení **IoT** s **umělou inteligencí (AI)**, nazývané **AIoT**. Zařízení nebudou data jen sbírat, ale budou schopna se samostatně rozhodovat přímo na místě (Edge AI) bez čekání na instrukce z cloudu.

Související články:

- Technologie 5G a mobilní sítě
- Kybernetické hrozby a bezpečnost
- Cloud computing a Edge computing

Tagy: network iot smart-home industry-4.0 sensors connectivity security

From:
https://serviceit.cz/ - **IT ENCYKLOPEDIE**

Permanent link:
https://serviceit.cz/doku.php?id=it:net:iot&rev=1767358880

Last update: **2026/01/02 14:01**