

Internet of Things

ultima frontiera nella rivoluzione di computazione e comunicazione; il termine si riferisce alla interconnessione che si sta espandendo dei dispositivi smart tramite cloud; concetto nato nel 1999 all'MIT

i dispositivi considerati appartenenti all'IoT sono:

- PC
- Smartphones
- ...
- tutti i dispositivi embedded (piccoli dispositivi con poca potenza di calcolo)

evoluzione dell'IoT:

1. Information Technology → uso di PC, server, router etc. acquistati da utenti e aziende per processare dati
2. Operation Technology → uso di macchine capaci di fare certe operazioni (es. braccio robotico che avvita una vite nella macchina nella catena di montaggio)
3. Personal Technology → uso di dispositivi da portare con sé (es. smartphone, tablet, eReader...)
4. Sensor/Actuator Technology → uso di dispositivi single-purpose acquistati da utenti, aziende di IT e di OT

Componenti di dispositivi IoT:

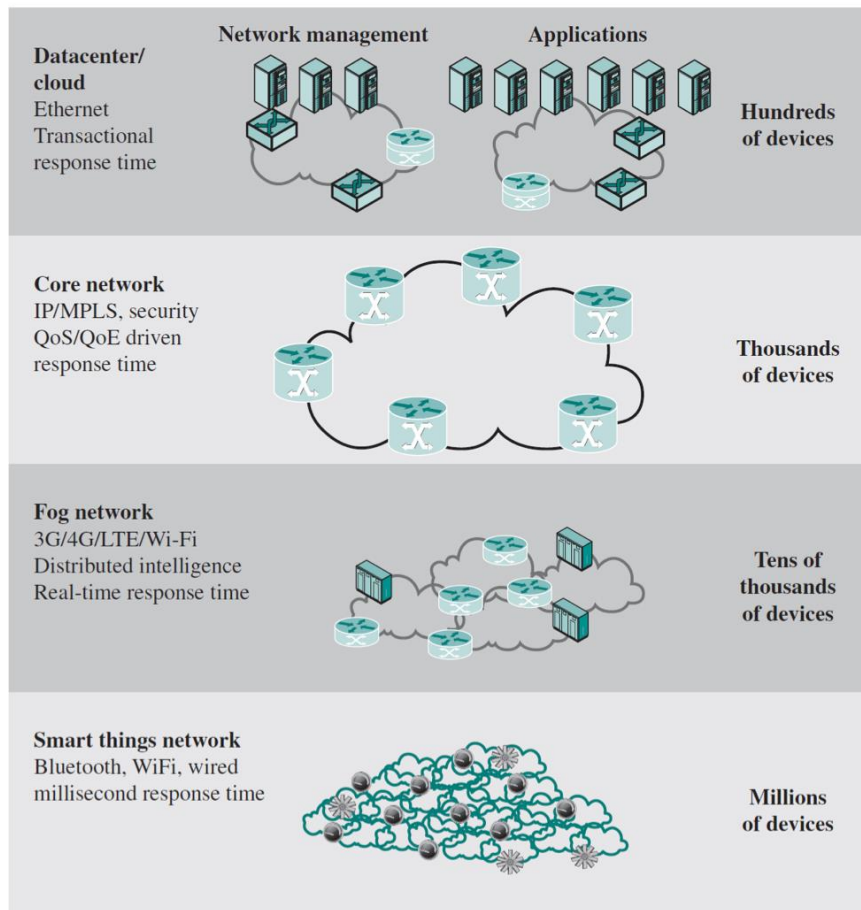
- Sensori → misura dei parametri fisici, chimici, biologici e invia segnali elettrici (tipicamente vengono inviati a microcontrollori)
- Attuatori → riceve un segnale elettrico da un controllore e risponde interagendo con l'ambiente per produrre degli effetti su un parametro fisico, chimico o biologico
- Microcontrollore → ciò che rende i dispositivi "smart"
- Ricetrasmittitore → contiene i componenti elettronici necessari per trasmettere e ricevere dati (di solito wireless)
- Radio-Frequency Identification (RFID) → uso onde radio per identificare gli oggetti

➔ l'IoT può essere visto come una grande rete formata da dispositivi e computer connessi tramite una serie di tecnologie intermedie

Nella struttura della rete IoT ci sono:

- Tagging things → oggetti che possono essere tracciati tramite RFID
- Feeling things → oggetti che fanno da sensori
- Shrinking things → oggetti molto piccoli (nanotecnologie)
- Thinking things → oggetti che hanno potere decisionale e capacità di calcolo

In un'azienda avremo:



Per i dispositivi embedded, il sistema operativo deve essere fatto ad hoc perché sono dispositivi limitati (poca RAM, poca batteria, no unità di gestione di memoria e performance del processore limitato); es. TinyOS, RIOT, μ Clinux

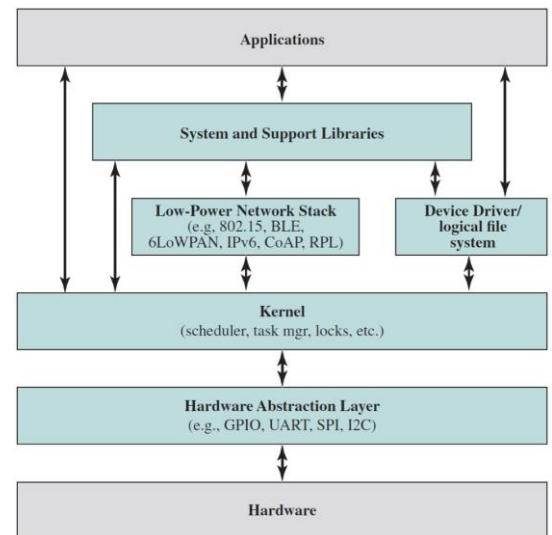
Requisiti per sistema operativo di un dispositivo IoT:

- poca memoria → sia ROM che RAM; deve bastare sia per il sistema operativo che per le applicazioni; librerie e strutture dati ottimizzati
- supporto per diversi hardware
- connettività di rete → vari possibili protocolli di connessione tra cui:
 - IEEE 802.15.4 [low-rate wireless personal area network (WPAN)]
 - ZigBee
 - Bluetooth Low Energy (BLE)
 - 6LoWPAN (IPv6 over Low-power Wireless Personal Area Networks)
 - CoAP (Constrained Application Protocol)

- RPL (Routing Protocol for Low power and Lossy Networks)
- LoRaWAN (low-power Long-Range network technology)
- efficienza energetica
- supporto di funzioni real-time
- sicurezza → può essere fornita su vari layer; la sicurezza non è però implementata bene quindi sono dispositivi facilmente hackerabili

La struttura tipica di un dispositivo IoT è formata da:

- hardware e livello di astrazione (per supporto di hardware diversi)
- kernel
- device driver
- low power network stack (per connettività di rete)
- applicazione e librerie di supporto (comunica con il kernel per motivi di efficienza)



Guardando alle caratteristiche di alcuni sistemi operativi, notiamo che μ Clinux non è low-power perché ha richieste di RAM e di ROM con ordini di grandezza più alti rispetto agli altri; la modularità è importante per i sistemi IoT ma per un utente non esperto rende difficile l'installazione e la configurazione

	μ Clinux	TinyOS	RIOT
Minimum RAM	< 32 MB	< 1 kB	~1.5 kB
Minimum ROM	< 2 MB	< 4 kB	~5 kB
C Support	✓	✗	✓
C++ Support	✓	✗	✓
Multithreading	✓	○	✓
Microcontrollers without MMU	✓	✓	✓
Modularity	○	✗	✓
Real time	○	✗	✓

✓ = full support
○ = partial support
✗ = no support

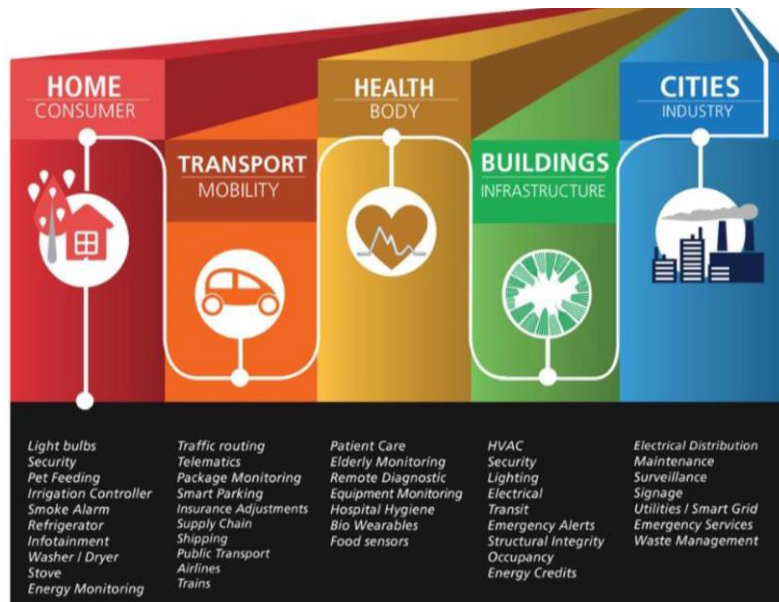
Attualmente ci sono più dispositivi che persone sulla terra (circa 13 dispositivi connessi ad Internet/persona)

i dispositivi IoT vengono ormai utilizzati in molti campi (trasporto, educazione, casa, business, energia, controlli ambientali...) e le varie entità sono tutte connesse tra di loro → ci sono scambi di informazioni ⇔ otteniamo reti individuali che possono comunicare tra di loro (permette studi analitici statistici di gestione)

Nel futuro si parlerà di città completamente automatizzate (es. ferrovia smart, l'ospedale smart, la centrale elettrica...) e usando tutti i dispositivi connessi e le

informazioni derivanti da essi, si possono pianificare le attività di ogni componente funzione delle altre e ottimizzare i consumi (circa \$150 miliardi tra le varie industrie)
→ **Industrial Internet**

Le applicazioni di dispositivi IoT sono volte ad automatizzare la vita dei consumatori; ci sono tantissimi campi applicativi:



altri esempi → shopping, blockchain delle mucche, monitoraggio del sonno, controllo tramite pensiero

Tutto questo genera una grande quantità di dati (**Big Data**)

Le critiche verso l'uso di dispositivi IoT sono legate all'aspetto etico e di sicurezza dei dati → un'azienda controllando la temperatura di una stanza potrebbe raccogliere dati su quando l'utente è a casa; se questi dati vengono violati l'utente è potenzialmente a rischio; inoltre, questa può essere considerata come una violazione della privacy (aspetto etico)