Sintesi

Introduzione all'IoT

Con ***Internet of Things*** si intende l'estensione del concetto di Internet al mondo degli oggetti e luoghi concreti.

Gli **oggetti (smart)**:

1. si rendono riconoscibili (identificazione);
2. comunicano dati su loro stessi (connessione);
3. accedono a dati o informazioni aggregate di altri (capacità di elaborare dati).

In particolare, risulta rilevante la problematica della **sicurezza e privacy**: qualsiasi tipo di *device*, essendo connesso ad una rete, diventa un punto di attacco potenziale. Le regole base per prevenirlo sono **password** e **cifratura**.

Per poterlo comprendere il mondo dell'IoT, è necessario conoscere alcuni elementi:

- **sensori**, dispositivi input di rilevamento che raccolgono informazioni dall'ambiente fisico;
- **attuatori**, dispositivi output per controllare un processo, seguire un'azione o influenzare le condizioni dell'ambiente esterno;
- **microcontrollori,** dispositivi elettronici integrati su singolo circuito elettronico che contengono RAM, CPU e tutto ciò che serve a svolgere le funzionalità tipiche di un microprocessore per pc, ma in sistemi *embedded* (per applicazioni specifiche di controllo digitale);
- ***gateway***, un nodo centrale che raccoglie i dati e permette di utilizzare al minimo le risorse per la comunicazione;
- ***carrier*****,** il tipo di rete che permette la connessione ad internet e trasferimento di dati (vedi Wi-Fi, 5G, etc.) ad un *server* di *storage* che, a sua volta, organizza i dati e li fornisce agli output.

Il paradigma che sta dietro l'IoT è quello di avere **Agenti Intelligenti**. Essi possono seguire diversi modelli di calcolo:

- *Edge computing.* Si tratta di un modello distribuito dove l'elaborazione dei dati avviene più vicino possibile a dove i dati vengono richiesti (in prossimità del sensore). È largamente **adottato nell'ambito dell'IOT**;
- *Cloud computing.* Si tratta di un paradigma di erogazione di servizi offerti su richiesta da un fornitore a un cliente finale attraverso la rete internet (come l'archiviazione, l'elaborazione o la trasmissione dati). È usato per i **dati meno 'time-sensitive'**.

Reti di telecomunicazioni

Internet of Things è da considerarsi come una rete di telecomunicazioni. Ma cosa sappiamo di queste ultime?

Partendo dalle origini di **Internet** (rete di dati), nato dall'elitario Arpanet (con il protocollo IP), ed arrivando all'attuale www, ovvero protocollo *http* per la connessione, in questa dispensa si racconta l'evoluzione della **rete di dati** e, in parallelo, di quella **telefonica**. La rete telefonica presenta come requisito fondante l'interattività e come caratteristica principale (relativa alla variante digitale) un bit rate variabile che ha comportato, negli anni, una

spasmodica ricerca di alternative al collegamento classico (**commutazione di circuito**), in quanto poco efficiente.
La soluzione trovata è la **commutazione a pacchetto** (adatta sia alla rete di dati che alla rete telefonica grazie al *Voice over IP*), che può però comportare congestione dei buffer di dati, motivo per cui risulta necessario il controllo di congestione (*Congestion Control*). Questo aspetto rischia di inficiare l'interattività: infatti, per lungo tempo, la soluzione è stata utilizzata solo per la rete di dati tra calcolatori (internet) e non per i telefoni, dove tale requisito è fondamentale.

In questo contesto, è dunque necessario specificare che l'IoT M2M *Communication*, ma di una **rete**, un'**infrastruttura globale che abilita nuovi servizi avanzati grazie all'interconnessione di oggetti fisici e virtuali.**

Si giunge a parlare delle **reti mobili**, in particolare della tanto discussa **rete 5G**, ultima evoluzione: è una rete fortemente densificata, con banda larga ad 1 Gbit, ritardo di trasmissione ridotto a 1 millisecondo e permetterà il *massive IoT* (1 milione di dispositivi per ogni metro). Tutti questi progressi sono resi possibili dai **due nuovi paradigmi delle telecomunicazioni**: *software define networking* (separazione sosftware e hardware) e *network function virtualization* (macchine virtuali che girano su data centre).

Infine, nella presente dispensa vediamo anche alcune applicazioni di IoT:

- *Intelligent trasportation service* (geometrie variabili e applicazioni di fluidodinamica al mondo dell'automotive);
- *Precise Agricultural Production* e in particolare LoRaWAN, soluzione dell'azienda Natech.

Introduzione a Zerynth
Zerynth, startup innovativa che offre una **piattaforma IoT** basata su programmazione dei microcontrollori con linguaggio python, mostra il proprio punto di vista sull'argomento, ponendo l'accento sulla distinzione importante tra linguaggio di programmazione di basso livello (C++, Assembly, etc) e di alto livello (Java, python, Java Script), il quale è più vicino al linguaggio naturale (commentato e ordinato).

La piattaforma Zerynth presenta la funzione di **ponte** tra hardware (ad esempio il suo *4zerobox*) e cloud (*zdm*), abilitando anche una serie di servizi resi da terze parti (quali il servizio di creazione di dashboard dai dati raccolti, fornito da Ubidots).
Nella parte *hands-on* della lezione, sono stati fatti vari esercizi step-by-step (con devicefisico per chi era in aula e virtuale per chi era online).

Internet of Things

Introduzione all'IoT: gli elementi di base

Il termine "*Internet of Things*" (**IoT**) è nato da un ricercatore, Kevin Ashton, nel 1999: inizialmente, consisteva nel dare una maggiore capacità ai computer in modo che potessero, in qualche modo, vedere e sentire il mondo. Nel corso del tempo la definizione è stata **raffinata** e sono stati definiti i **principi** alla base: esistono degli oggetti che devono essere riconoscibili (**identificazione**), devono avere la capacità di comunicare dati su loro stessi (**connessione**) e devono poter accedere a dati aggregati di altri dispositivi (**capacità di elaborare i dati**).
Questi sono perciò i presupposti per considerare gli oggetti come ***smart object*** (dispositivi, apparecchiature, impianti e sistemi, materiali e prodotti tangibili, opere e beni, macchine e attrezzature).
Tali oggetti possono essere applicati in diversi contesti: Smart Home/Building, Smart Factory, Smart City, Smart Car, etc. Inoltre, le possibilità di connessione degli smart objects sono diverse:

- A corto raggio
- A lungo raggio (ad esempio utilizzando il 4G e il 5G)

Il settore IoT, attualmente, possiede una grande rilevanza: il suo mercato risulta in costante espansione (in Italia si stimava già dal 2019 che valesse 6,2 Miliardi di euro).

Una premessa: sicurezza e privacy

Un tema importante riguardante l'IoT è relativo alla **sicurezza e privacy**: è sicuramente necessario avere consapevolezza su quali sono i vantaggi nell'introdurre nuove tecnologie, ma anche sapere come trattare aspetti legati alla privacy nel momento di introduzione dei dispositivi IoT, Infatti,
si ricevono in continuazione notizie relative ad attacchi informatici nei confronti di numerose aziende attraverso dispositivi IoT in quanto questi ultimi sono fonti di ingenti moli di dati.

"...negli ultimi tre anni qualcosa come un'azienda su 5 ha subito almeno un attacco ai propri ambienti Internet of Things" (società di ricerca Gartner nello studio "Worldwide IoT security spending forecast 2018-2021 per segment").

Qualsiasi tipo di **device**, essendo connesso ad una rete, diventa un **punto di attacco potenziale**.
Da tale aspetto conseguono, perciò, alcune **regole base** per prevenirlo:

- Password e metodi di autenticazioni robuste;
- Cifratura (encryption).

Bisogna, in sintesi, avere consapevolezza dei limiti e possibilità di protezione dall'esterno, tenendosi sempre aggiornati su quelli che possono essere nuovi rischi poiché è un mondo molto dinamico.
Bisogna quindi fare in modo che tutte le componenti hardware abbiano sempre le componenti software aggiornate al fine di assicurare la massima protezione e il massimo livello di privacy.

Inoltre, anche i ***dispositivi di storage*** devono essere protetti da accessi indesiderati, non solo i ***device per acquisire i dati.***

Perciò, con l'aiuto di esperti, dopo *attacchi a dispositivi IoT*, bisogna analizzare questi ultimi per implementare accorgimenti, in modo da evitarlo nel futuro.
I **dispositivi IoT** spesso sono **sottovalutat**i, si pensa che siano dispositivi sensoriali passivi: rappresentano, invece, dei prolungamenti di capacità percettiva delle persone!
In questo senso possono essere visti come strumenti che possono portare ad avere un **occhio all'interno di un ambiente** in cui fisicamente non si può essere. Costando poco, possono sembrare davvero semplici oggetti, ma son sempre **punti di ingresso**.
Esistono, perciò, numerose *strategie*: ad esempio, nel caso di una rete aziendale molto ampia con tanti dispositivi connessi tra di loro, si potrebbero creare delle **sottoreti**, in modo tale che, se avviene un attacco, si limita ad una certa porzione di rete. Da tale soluzione deriva, però, il rovescio della medaglia: a volte non si tiene a mente che l'attacco ad una parte della rete poco importante rischia di compromettere tutto il resto perché si sottovaluta l'attacco, ritenendolo poco significativo.

Nell'ambito industriale, come vedremo nei paragrafi successivi, l'IoT riporta diverse **applicazioni (I-IoT)**:

- **Smart Factory**: permette il controllo della produzione in maniera avanzata, di implementare procedure di sicurezza sul lavoro con prezzi bassi e con grande pervasività, di gestire le merci e i rifiuti;
- **Smart Logistics**: risulta utile per la tracciabilità e monitoraggio della filiera tramite tag RFID (Radio-Frequency Identification) e sensoristica, monitoraggio della catena del freddo, gestione della sicurezza in poli logistici complessi, gestione delle flotte (ad esempio tramite GPS / GPRS)
- **Smart Lifecycle**: consente il miglioramento del processo di sviluppo di nuovi prodotti (ad esempio tramite dati provenienti da versioni precedenti dei prodotti connessi), end-of-life management e la gestione fornitori nella fase di sviluppo nuovi prodotti.

I dati che vengono acquisiti devono essere spesso rielaborati per **estrarne altre informazioni.**
Esempio: Google Maps è una raccolta dati in un certo istante utile ad avere informazioni geografiche e sul traffico, ma anche ad avere *trend* di evoluzione del traffico. I sensori in questo caso sono i tanti cellulari a cui accede Google che inviano informazioni sulla loro posizione e, in base alla velocità di spostamento, vengono ricavati dei modelli di traffico.
Esempio: esistono vasetti di medicine con sensori posti sulla chiusura o su un blister per verificare se viene aperto al fine di prelevare la pillola, così da permettere che l'operatore medico abbia consapevolezza se quella medicina è stata assunta dal paziente e, eventualmente, intraprendere operazioni per ricordare o chiedere al paziente di seguire le prescrizioni mediche.

A seguire si riportano le **caratteristiche** (**capacità chiave**) degli **oggetti *smart***:

1. Poter rielaborare le informazioni
2. Comunicare in modalità bidirezionale
3. Essere riconfigurabili
4. Intraprendere azioni conseguenti ad eventi
5. Trasmettere dati in *real-time,* ovvero in tempo reale

Esistono una serie di **casi attual**i e **attuati** di intelligenza aggiunta a vari contesti, di cui riportiamo alcuni esempi conosciuti:

- Il monumento che comunica al turista informazioni sulla sua storia, abilitando ricostruzioni virtuali;

- L'autovettura che, comunicando i suoi dati sul tipo di guida, permette di fornire informazioni non solo per il monitoraggio del traffico, ma anche dati utili alle assicurazioni per capire la dinamica di un incidente;
- Contatori di tipo digitale in casa che, evitando la lettura fisica, forniscono l'entità dei consumi, dalla quale si possono ricavare le abitudini dell'utente.

In tutti questi casi ci sono diverse **problematiche**:

- Costi ingenti;
- Problemi di privacy e sicurezza;
- Implicazioni derivanti da un utilizzo non efficiente dei dispositivi.

Definizioni e tipologie

Vediamo in questo sotto-paragrafo alcune definizioni cardine del mondo IoT.
I **sensori** sono dispositivi di rilevamento che raccolgono informazioni dall'ambiente fisico in cui si trovano.
Gli **attuatori** sono dispositivi per controllare un processo, eseguire un'azione o influenzare le condizioni dell'ambiente esterno in cui si trovano.
In alcuni casi i dispositivi periferici rivestono il **duplice ruolo** di **dispositivi di rilevamento** e di **azionamento** per raccogliere dati dell'ambiente fisico ed effettuare il controllo.

Sensori SMART
Le **caratteristiche** chiave sono le seguenti:

- Tecnologia di *sensing*: determina il tipo di dato o dati rilevabili e le prestazioni ottenibili;
- Alimentazione: fattore principale che determina l'autonomia e la durata di funzionamento del dispositivo, la sua collocazione e alloggiamento nell'ambiente;
- Elaborazione e memoria: dipendono dall'intelligenza richiesta per determinare i dati desiderati in uscita e le capacità di mantenere una collezione di misure e informazioni (anche esterne) nel tempo. Si può fare una rilevazione a intervalli diversi, perciò il meccanismo di memoria potrebbe permettere di vedere, ad esempio, un intero pacchetto o gli ultimi dati.
- Comunicazione: deve essere possibile stabilire una comunicazione affidabile, sicura e protetta per mezzo della rete.

Immaginiamo ora di dislocare nell'ambiente diversi **dispositivi a basso costo** (che possono misurare informazioni e parametri variegati).