CAMERA DI COMMERCIO
DEL MOLISE

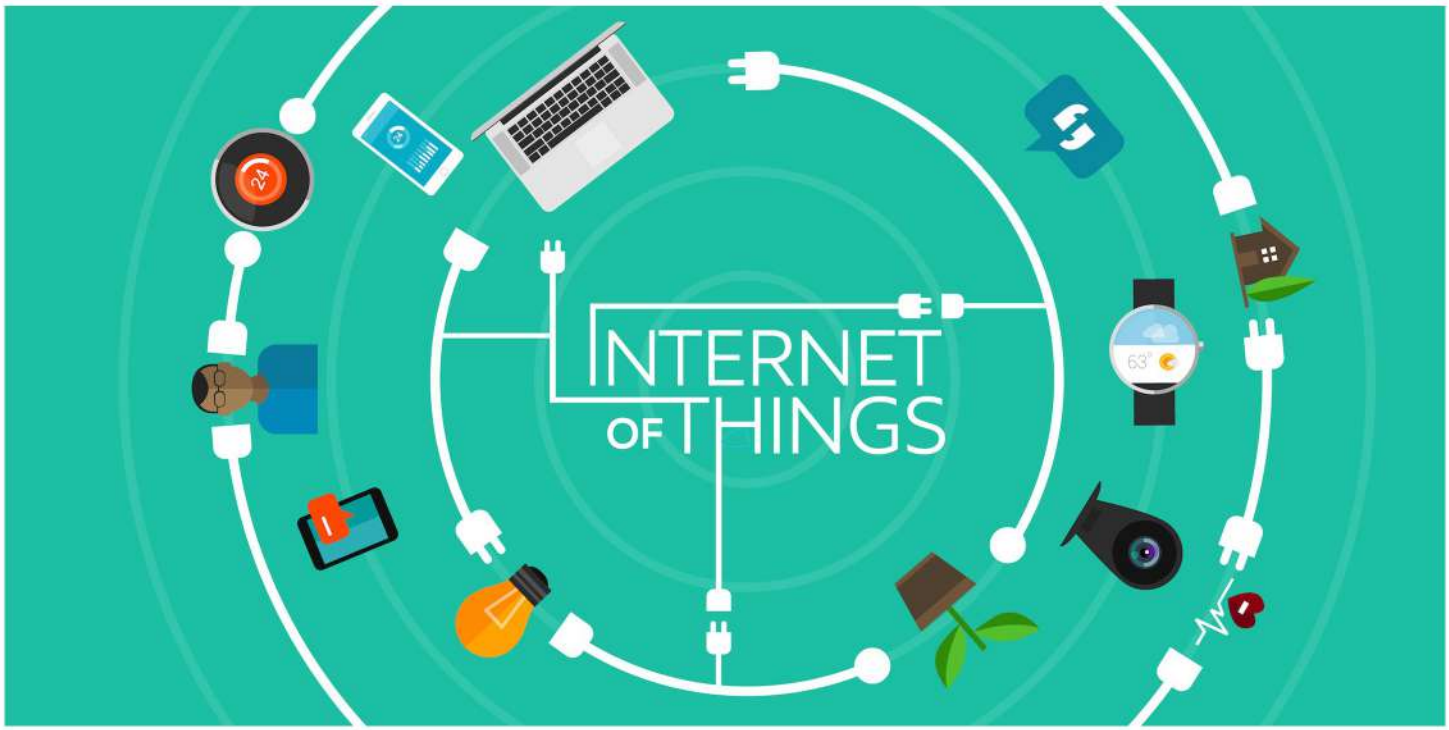
punto
impresa
digitale

Le guide
per l'innovazione
digitale

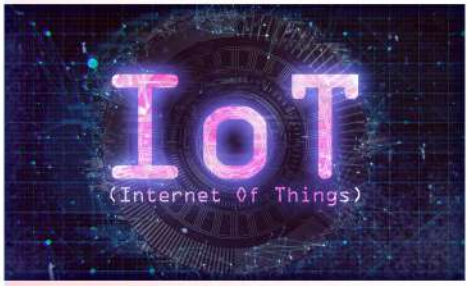
numero 5

Internet of things

Scopri di più su Internet of things



Internet of things



Con il termine “Internet of Things” (IoT)si indica “un insieme di tecnologie che consentono di collegare a Internet qualunque tipo di apparato al fine ultimo di trasferire informazioni”. Aumenta la diffusione dell’internet delle cose e pertanto si assiste ad una rapida crescita: in Italia è presente una forte fiducia verso le tecnologie IoT più consolidate e i dispositivi connessi. Qualunque sia la connessione, non avviene più soltanto tra computer, ma fra una vasta gamma di oggetti o cose, infatti tutto può entrare a far parte della IoT. Ciò che occorre è creare qualche circuito elettronico per rendere possibile il collegamento stesso tra gli oggetti e lo scambio di informazioni. Attraverso il Rfid (Identificazione a radio frequenza) e il QR code, si può dare una “identità elettronica” a tutto quanto ci circonda nella vita reale: tag, chip e sensori consentono di trasformare un oggetto analogico in un dispositivo “smart”.

- **RFID (Radio-Frequency IDentification)**: si intende una tecnologia per l'identificazione e/o memorizzazione automatica di informazioni inerenti ad oggetti, animali o persone basata sulla capacità di memorizzazione di dati da parte di particolari etichette elettroniche, chiamate tag e sulla capacità di queste di rispondere all'interrogazione a distanza da parte di appositi apparati fissi o portatili, chiamati reader.

- **QR code**: è un codice a barre bidimensionale (o codice 2D), ossia a matrice, composto da moduli neri disposti all'interno di uno schema bianco di forma quadrata. Viene impiegato per memorizzare informazioni generalmente destinate a essere lette tramite uno smartphone.

Si pensi alla tradizionale sveglia che si trasforma in un oggetto “smart” che consente di avvisarci in tempo ed interagisce con il mondo circostante: reperisce e trasferisce informazioni tra mondo reale e quello virtuale.

1.Ambiti di applicazione dell’IoT e casi d’uso per consumatori e aziende

Monitorare, controllare e trasferire informazioni è l’obiettivo di questo tipo di tecnologia fondamentale, per poi compiere azioni conseguenti.
Il significato di IoT può essere ancor più compreso attraverso degli esempi:

- **Smart City (città intelligenti)**

Per migliorare la qualità della vita in città, cercando di andare incontro alle esigenze e ai bisogni dei cittadini ci sono le Smart City, ossia “le città intelligenti” o “città sensibili”.
I semafori intelligenti, che dal rosso passano al verde, quando le autovetture non percorrono la strada nel senso opposto, sono un esempio di tecnologie adottate per realizzare città intelligenti; così come i sistemi innovativi per la gestione e lo smaltimento dei rifiuti oppure le innovazioni ambientali, energetiche, di mobilità, comunicazione, ed urbanistiche.

Tra i settori sui quali si assiste a un maggior interesse a livello industriale e di pubbliche amministrazioni rileviamo tutto il mondo delle Smart City che si accompagna con tematiche legate ai progetti della pubbliche amministrazioni e ai temi più strategici come quelli relativi agli Open Data.

- **Smart Building e Smart Home (case e palazzi connessi)**

Si rivolgono ai consumatori finali dei servizi le smart home, ossia le case intelligenti: un esempio può essere la temperatura della casa che si può regolare a distanza oppure il rilevamento delle persone in appartamento attraverso i sensori. Gli smart building (edifici intelligenti), invece, si rivolgono soprattutto al B2B (Business to Business), ovvero alla realizzazione ed ottimizzazione di palazzi ed uffici, per dotarli di oggetti intelligenti che interagiscano con l'ambiente interno (ad esempio gestione della luce e dell'energia elettrica).

- **Smart Mobility**

La premessa per avere una Smart City è l'esistenza della Smart Mobility; infatti, per determinare la qualità della vita delle nostre città il tema della mobilità è assolutamente centrale. Molte sono le aziende che si stanno avvicinando a questo ambito, in quanto, nella dimensione delle Smart Car e della Connected Car e nelle applicazioni legate al mondo del trasporto ferroviario con treni controllati da IoT, si aprono grandissime opportunità di business.

- **Smart Agriculture**

Attualmente l'Agrifood è uno dei settori con la più elevata opportunità di sviluppo e con la più bassa introduzione di soluzioni digitalizzate.
Si tratta di un settore che a livello di sensoristica ambientale e territoriale, di applicazioni per il meteo, di automazione di apparati per la gestione sempre più precisa di acqua, fertilizzanti, concimi, agrofarmaci necessita di soluzioni digitali.
Le esperienze sono tante e legate all'utilizzo dei droni, a sensoristica che rimanda ai temi dell'Internet della Terra, a soluzioni di logistica innovativa per la Smart Agriculture, o ancora a soluzioni per l'agroenergy o a operazioni che puntano a migliorare il rapporto legato a cibo e sostenibilità.

- **IoT e Pubblica amministrazione: trasporti, energia, sostenibilità, rifiuti, ambiente**

Un ruolo fondamentale per lo sviluppo dell'Internet delle cose, oggigiorno, è ricoperto dalle Pubbliche Amministrazioni. Infatti, con molta più frequenza la tecnologia è regolamentata, finanziata e gestita dal settore pubblico anche nella prospettiva dell'Intelligent Transport System (ITS). Un esempio significativo di quanto appena esplicitato è l'introduzione obbligatoria dei contatori intelligenti per il telecontrollo e la telegestione.
Il soggetto pubblico può e deve promuovere azioni di indirizzo stanziando finanziamenti straordinari destinati a enti pubblici e aziende private: ciò può accadere ad esempio per la riduzione dei consumi energetici o per la sostenibilità delle aree urbane. Infine il soggetto pubblico spesso è anche committente: è il caso dell'Internet of Things utilizzato per l'illuminazione stradale o per il monitoraggio preventivo del territorio.

- **Smart Manufacturing (industria 4.0 o industry 4.0)**

La smart manufacturing trae vantaggio da avanzate tecnologie dell'informazione e della produzione per consentire la flessibilità nei processi fisici e per affrontare un mercato dinamico e globale. In quest'ottica, il ruolo svolto dall'Internet of Things è di vitale importanza.

Dalla macchina a vapore ai macchinari intelligenti che si autoprogrammano, l'obiettivo strategico nelle industrie manifatturiere è sempre stato quello di migliorare l'efficienza dei processi. Questo oggi è possibile grazie agli approcci di Smart Manufacturing e Industrial IoT. I dati acquisiti senza soluzione di continuità, dal produttore delle materie prime fino al consumatore, offrono alle aziende moderne l'accesso a nuove capacità analitiche avanzate che trasformano una base informativa di dati grezzi (i cosiddetti Big Data) in una fonte preziosissima di informazioni necessarie a migliorare i prodotti e i servizi supportando al meglio i processi decisionali in azienda.

3. I gradi di maturità e le applicazioni IoT per business e società

Esistono 3 gradi di maturità: applicazioni consolidate, applicazioni sperimentali e applicazioni embrionali, secondo le quali gli ambiti applicativi dell'Internet delle cose possono essere suddivisi. In Italia le applicazioni consolidate coincidono con le più semplici, le applicazioni attualmente in fase sperimentale sono quelle che più si avvicinano al paradigma dell'Internet of Things e le embrionali sono i progetti per il futuro.

a) Applicazioni IoT consolidate

Nel nostro Paese, le soluzioni più semplici e di immediata realizzazione riguardano determinate applicazioni, quali: la videosorveglianza e la sicurezza nelle smart home finalizzata al controllo e all'antintrusione o alla gestione delle flotte aziendali; la tracciabilità degli oggetti di valore così come il monitoraggio del traffico cittadino in ambito smart city.

Altri esempi sono: i contatori intelligenti (smart meetering) per misurare i consumi, le soluzioni domotiche, la sicurezza delle persone, i servizi di infomobilità e la registrazione dei parametri di guida. Il mercato di queste soluzioni applicative nel nostro Paese procede lentamente, ma lavorando e ragionando sul valore reale che producono a lungo termine, sarà possibile raggiungere la loro diffusione in breve tempo. Perché questo accada è necessario che le aziende ridefiniscano le strategie di comunicazione con i potenziali utenti.

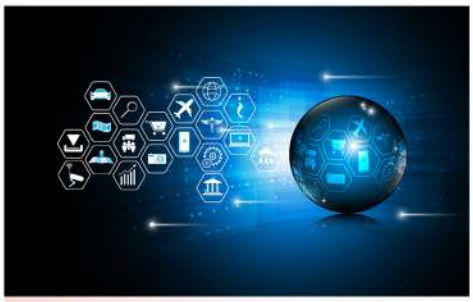
b) Applicazioni IoT sperimentali ed embrionali

In Italia hanno difficoltà a svilupparsi tutte quelle soluzioni basate su tecnologie RFId per la supply chain (diverse attività logistiche delle aziende, con l'obiettivo di controllare le prestazioni e migliorarne l'efficienza), che sono alla base dell'Internet delle cose.

La stessa criticità si riscontra sulle tecnologie nell'ambito eHealth (IoT per salute e medicina), in cui il telemonitoraggio dei pazienti potrebbe ridurre drasticamente i costi ospedalieri.

4. Le fasi fondamentali dell'Internet delle cose

La fase definibile come pre-Internet of Things è rappresentata dalla sensoristica "semplice": dispositivi in grado di effettuare data collection in modo sempre più preciso e mirato in funzione di specifici ambiti applicativi (apparecchiature dedicate a rilevare dati legati alla temperatura di ambienti, al movimento di veicoli, alla qualità dell'aria, al livello di rumorosità di determinati ambienti o alla presenza di determinate sostanze).



Il passaggio dalla sensoristica all'Internet of Things è costituito appunto dalla connessione in rete. Conseguentemente si entra nell'Internet of Things ogni volta che abbiamo dispositivi connessi in rete:

- in grado di rilevare e comunicare dati ;
- in grado di rilevare più tipologie di dati e di trasferirli;
- in grado di effettuare un primo livello di elaborazione (selezione) dei dati a livello locale per trasferire solo quelli che corrispondono a determinati requisiti;
- in grado di raccogliere dati, effettuare un primo livello di selezione e di effettuare azioni in funzione di indicazioni ricevute;
- in grado di rilevare dati, di selezionarli, di trasmettere solo quelli necessari al progetto nel quale sono coinvolti, di effettuare azioni sulla base delle indicazioni ricevute e di effettuare azioni in funzione di una capacità elaborativa locale.

5.Elementi costitutivi dell'IoT

Per svolgere la propria funzione un dispositivo IoT ha bisogno di:

Sensori: che misurano proprietà fisiche (luce, umidità, movimento, pressione, temperatura…). Tali sensori sono: accelerometro, giroscopio, magnetometro, GPS, sensore di luce ambientale, barometro, sensore di prossimità ad infrarossi, sensore di impronte digitali, sensore di temperatura, microfono.

Attuatori: che muovono o controllano meccanismi usando sistemi elettrici, idraulici o pneumatici.

Controller: che riceve input dai sensori e prende decisioni per attivare gli attuatori.

Esistono tre tipi di mezzi utilizzati dai dispositivi IoT per comunicare:

- rame: è economico, facile da installare e presenta una bassa resistenza alla corrente elettrica. Tuttavia, è limitato dalla distanza e dalle interferenze del segnale.
- fibre ottiche: i cavi possono viaggiare a distanze significativamente più lunghe rispetto ai cavi in rame.
- wireless: esiste una vasta gamma di opzioni di connessione tra cui segnali elettromagnetici, frequenze radio e microonde e collegamenti satellitari.

6.Sicurezza IoT e Privacy

Quello della privacy e della tutela dei dati personali e sensibili è un altro punto importante dell'internet delle cose.
L'Internet delle cose sembra di facile accesso, in grado di semplificare la nostra vita, di trasformare in smart case, città, auto e anche l'energia. Il risvolto della medaglia è quello della privacy degli utenti. Si è già visto come molti IoT non rendano chiaro l'utilizzo dei dati dei loro fruitori e non permettano in maniera semplice la rimozione degli stessi.

Per affrontare il tema della sicurezza nell'IoT bisogna far sì che ogni dispositivo che introduce una connessione IP sulla rete, sia protetto prima di essere fisicamente collegato al network aziendale e ci deve essere l'aggiornamento periodico dei sistemi di protezione.
La strategia di sicurezza nell'IoT deve fare riferimento a una serie di punti irrinunciabili per garantire sicurezza ad ambienti, produzione, persone, elecati di seguito:

- **l'autenticazione dei device IoT**

Ogni nuovo device deve essere autenticato e autorizzato e quindi chiunque tenti di accedere alla rete aziendale deve essere sottoposto a un processo di autenticazione, con controllo degli accessi;

- **cifratura**

La rete deve fare affidamento ad un controllo sui dati condivisi da tutti i device e dalle applicazioni, ed è necessario trasmettere i record in sicurezza grazie a strumenti di cifratura;

- **archiviazione**

Anche la fase di archiviazione sui dispositivi storage deve essere svolta con grande attenzione e i sistemi di archiviazione devono disporre di sistemi di protezione analoghi a quelli dei sistemi di produzione;

- **aggiornamento di tutte le componenti software**

Qualsiasi tipo di apparato e di macchinario nelle imprese, nelle organizzazioni delle Pubbliche Amministrazioni, negli edifici, dispone di una componente software sempre più importante. Una buona governance di sicurezza deve prevedere una massima attenzione a tutti gli aggiornamenti, se alcune parti non vengono aggiornate in modo puntuale si corre il rischio di aprire dei varchi e di rendere inutile tutto il lavoro su altri ambiti;

- **analisi dei possibili attacchi**

Gli ambienti gestiti anche dall'IoT sono sempre più numerosi, complessi e molto più connessi. Sensori e apparati inviano di continuo dati rilevanti sulla sicurezza degli accessi, delle persone, degli impianti e sono degli entry point che possono permettere a malintenzionati di accedere, violare, sabotare, spiare le reti e le attività che vi si appoggiano. Ci sono purtroppo attacchi pensati specificamente per compromettere determinate aziende o determinate attività. E' pertanto necessario progettare e attuare forme di protezione personalizzate e specificatamente indirizzate a proteggere aziende anche da precise minacce;

- **rischi di sabotaggi**

Occorre anche assicurarsi che i device IoT siano costantemente monitorati e controllati per evitare tentativi di sabotaggio;

- **suddivisione della protezione in aree**

La protezione dai rischi per l'IoT non è univoca e assoluta. Una falla nella sicurezza di un device collegato alla rete può danneggiare l'intera rete aziendale. Ecco che la suddivisione della rete in aree del network permette di minimizzare i rischi riducendo la superficie d'attacco.

CAMERA DI COMMERCIO
DEL MOLISE

punto
impresa
digitale

Punto Impresa Digitale

Camera di Commercio del Molise

Piazza della Vittoria, 1 – 86100 Campobasso
Corso Risorgimento, 302 – 86170 Isernia

pid@molise.camcom.it Tel. 0874/4711
www.molise.camcom.gov.it