



LIBRO BIANCO SUL BUILDING DIGITALE IN UNO SCENARIO IOT: SFIDE E OPPORTUNITA'



ANIE BUILDING DIGITALE
LUGLIO 2020

Indice

Premessa	5
Introduzione e Ringraziamenti	6
Glossario dell'IoT e delle soluzioni digitalizzate	7
Cosa significa e le opportunità dell'IoT	10
Perché ora si parla di IoT: il contesto tecnologico globale	10
Storia di una evoluzione: da M2M a IoT	14
Anatomia di una soluzione IoT	17
Scalabilità dei sistemi IoT	23
L'avvento della Industry 4.0	25
Esempi di utilizzo di IoT	26
Il concetto di Digital Twin	28
Come estrarre valore dai dati prodotti dalle Cose connesse	29
Data economy e il significato dei dati	31
Le principali categorie di dati IoT	31
Localizzazione	32
Ambiente	32
Macchine	32
Salute	33
Movimento	33
Gli attori costituenti l'ecosistema	33
I generatori dei dati	33
I fornitori di data services	33
Data business user	34
I consumatori finali	34
Il valore dei dati nel tempo	34
Modelli di business	35
Dalla Sharing Economy all'Outcome Economy	36
Le norme della Sharing Economy	38
Esempi di uso dei dati: il caso dei dati prodotti dalle automobili	38
Il valore della Data Economy e le Norme	40
Elementi di Architetture IoT nell'Edificio	42
Gli strati dell'architettura	42
Generalità sui protocolli di campo negli Edifici	43

Panoramica sui protocolli di comunicazione e loro classificazione.....	45
Il Gateway un aggregatore che connette il campo al Cloud	47
Dagli IoT gateway in campo ai software gateway nel Cloud.....	48
Piattaforma di raccolta e di fruizione dei dati su Cloud tramite API.....	49
Building: Chi genera i dati e a chi interessano	52
L'estensione del concetto di Digital Twin al Building: una possibile evoluzione del BIM?	52
Il concetto di Servizio e di Applicazione per diverse tipologie di edifici	54
Servizi "orizzontali" o comuni ai diversi settori	54
Servizi che generano dati → BEMS	55
Servizi che generano dati → BACS	56
A chi interessano i dati e i relativi Servizi	56
Servizi "verticali"	59
Residenziale: esempi di Servizio, vantaggi e fruibilità	59
Uffici: esempio di Servizio, vantaggi e fruibilità	62
Centri Commerciali: esempio di Servizio, vantaggi e fruibilità	65
Ospitalità: esempio di Servizio, vantaggi e fruibilità	66
I dati, l'Edificio 4.0 e le normative di riferimento	68
Cybersecurity e privacy in un mondo digitale	72
Sicurezza nell'IoT	72
Privacy dei dati: raccolta, conservazione e diffusione	75
Le sfide e mercati dell'IoT "sicuro"	79
Sviluppare sistemi IoT "Sicuri"	80
Cosa valutare per rendere sicuro uno "sviluppo IoT"	80
Controlli di Security da tenere presenti nell'IoT.....	81
Alcune considerazioni ed aree da guardare con attenzione per la sicurezza IoT	81
Il mercato di riferimento del Building.....	84
Il mercato delle Costruzioni in Italia pre e post COVID-19.....	84
Fotografia pre emergenza sanitaria – investimenti 2019	85
Le previsioni per il 2020	86
L'Edificio Digitale: una opportunità di crescita per il settore.....	88
Appendice.....	90
Criteri di classificazione degli edifici.....	90
Esempi di classificazione degli edifici	93
Tassonomia degli elementi di un'architettura IoT	95

Brown Field e Green Field in architetture IoT	96
Gestione dei modelli di AI sul campo in architetture IoT.....	98
Indice delle Fonti	100
Indice delle Figure	102
Indice delle Tabelle	103



Copyright © 2020 Federazione ANIE

Tutti i diritti sono riservati. Ogni riproduzione, pubblicazione, diffusione è vietata senza autorizzazione di ANIE Federazione, Viale Lancetti 43, 20154 Milano.

Premessa

Il 2020 rimarrà nella memoria comune come l'anno della drammatica crisi pandemica dovuta al Covid-19, che ha travolto tragicamente il nostro Paese e il resto del Mondo, cambiato radicalmente le nostre abitudini e stili di vita.

La necessità di contenere la diffusione dei contagi ha richiesto il rispetto di rigide regole di distanziamento sociale, costringendoci nelle nostre case, spesso lontani fisicamente dagli affetti, in uno stato di sospensione delle attività economiche, culturali, scolastiche, sociali, con pesanti ripercussioni da gestire sia nell'immediato che nei prossimi anni. E' tempo di reagire, sperimentando con azioni concrete un approccio resiliente, che dalle difficoltà ci consenta di vedere e cogliere le opportunità, che dall'esperienza vissuta ci guidi verso politiche lungimiranti, moderne, orientate alla crescita e alla sostenibilità.

ANIE, forte di una base associativa composta da imprese per le quali la costante e continua innovazione tecnologica rappresenta il principale fattore di competitività, guarda da tempo con interessata attenzione al fenomeno della digitalizzazione, che apre a scenari nuovi di interazione delle persone tra di loro o con gli oggetti e con gli ambienti, che crea "valore" dai dati e informazioni digitali, con il consolidarsi di diversi modelli di mercato che presentano grandi potenzialità ma anche processi nuovi da gestire e regolamentare: uno su tutti "privacy e sicurezza dei dati". E mai, come in questo periodo, abbiamo percepito come e quanto la tecnologia può aiutarci a corrispondere alle esigenze del nostro vivere quotidiano, a ridurre le distanze, a lavorare, a studiare, a socializzare, e quanto la sua assenza o inadeguatezza possa essere penalizzante.

Il Libro Bianco ANIE sul *"Building Digitale in uno scenario IoT"* pone importanti spunti di riflessione nello scenario attuale, ma nasce ben prima dell'avvio della situazione di emergenza, con l'obiettivo sia di supportare le imprese, soprattutto le PMI, nell'affrontare una transizione digitale che riguarda in prima battuta le aziende stesse, chiamate a ripensare la loro offerta sul mercato e i propri modelli di business, ma anche dall'ambizione di contribuire ad alimentare un confronto con le istituzioni e all'interno delle filiere per condividere esigenze, aspettative, necessità e creare le condizioni favorevoli per un ammodernamento dei nostri edifici e delle nostre abitazioni in chiave digitale e circolare. Il Libro Bianco è il primo, importante passo di un progetto di ANIE ampio, ambizioso e stimolante, con filoni di attività specifiche in corso sulla certificazione "digitale" dell'edificio, sull'adeguamento tecnologico ai fini di maggiore sicurezza e comfort, sul tema della cybersecurity e dell'intelligenza artificiale nel contesto Edificio. Siamo pronti alla sfida, che ci auguriamo sarà accolta da tutti gli attori interessati a traguardare gli edifici nazionali in una prospettiva di modernità.

Vice Presidente con delega al Building

Filippo Girardi

Introduzione e Ringraziamenti

Se mi chiedessero di scegliere cinque parole per descrivere di cosa parla il *Libro Bianco ANIE sul Building Digitale in uno scenario IoT* direi: “Connessioni, Interconnessioni, Dati, Opportunità, Mercato”. Il Libro Bianco, infatti, nel fotografare uno scenario tecnologico in costante ma progressiva evoluzione, sempre più incentrato sul valore e uso dei dati, offre al lettore una analisi del processo di trasformazione in atto, processo che non è solo tecnologico o industriale ma anche sociale.

L’Internet delle Cose è già entrato nel nostro quotidiano, come conferma l’aggiornamento 2020 del Cisco Annual Internet Report, che stima che circa due terzi della popolazione mondiale disporrà entro il 2023 dell’accesso ad internet, con un numero di dispositivi connessi alla rete vicino ai 30 miliardi, ossia più di tre volte la popolazione mondiale. La medesima dinamica che negli anni passati ha caratterizzato l’avvio della transizione 4.0 nei processi industriali si sta quindi manifestando, forse con minore consapevolezza ma in maniera altrettanto dirompente, nel vivere quotidiano, influenzando le relazioni ed interazioni delle persone tra di loro, con le cose, con gli ambienti, con le istituzioni ed organizzazioni, con l’obiettivo di rispondere alle esigenze di ognuno in modo più semplice ed efficace.

Ma cos’è l’IoT e come sta diventando parte delle nostre vite? Il Libro Bianco ANIE sul “*Building Digitale in uno scenario IoT*” racconta le origini di ciò che a tutti gli effetti si pone come un nuovo paradigma di sviluppo tecnologico, come di consueto indirizzato da bisogni esistenti, emergenti o immaginabili, basato sulla capacità di raccogliere, trasferire, gestire e processare una mole crescente di dati e informazioni. La prima parte del volume declina il concetto della logica IoT quale parte integrante dei prodotti e apparecchiature offrendo, in tal caso soprattutto alle imprese, gli elementi necessari per sviluppare la rispettiva offerta in chiave digitale, contribuendo a formare un nuovo punto di vista sull’utilizzo e monetizzazione dei dati e su come questi possano contribuire alla definizione di nuovi modelli economici, più competitivi e sostenibili. La seconda parte, adatta anche al lettore comune, descrive come il processo di digitalizzazione si applica agli edifici e individua benefici e opportunità per le persone, come risposta concreta a esigenze anche diverse, a seconda del periodo della propria esistenza o delle condizioni di vita.

Il Libro Bianco ANIE è prima di tutto il frutto di un confronto costruttivo, appassionante, visionario, a tratti animato che ha coinvolte prima di tutto le imprese di ANIE e che si è arricchito nel tempo delle riflessioni di ANIA – Associazione Nazionale per le Imprese Assicuratrici – con il contributo di alcuni suoi associati, del Politecnico di Milano, di service provider.

Un ringraziamento sentito a tutti gli esperti che hanno messo a disposizione il loro tempo ed esperienza per la redazione del volume, allo staff di ANIE per il coordinamento e la messa a punto del Libro Bianco, e un particolare ringraziamento all’Ing. Tommaso Prini, che ha fortemente voluto la costituzione del Gruppo ANIE Digitale Building, intuendo i segnali di un cambiamento in atto da trasformare in opportunità.

Coordinatore Gruppo ANIE Digitale Building

Roberto Siagri

Glossario dell'IoT e delle soluzioni digitalizzate

M2M: Con M2M, acronimo di Machine-to-machine, in generale ci si riferisce a tecnologie ed applicazioni di telemetria e telematica che utilizzano le reti wireless. Machine-to-machine indica anche un insieme di software ed applicazioni che migliorano l'efficienza e la qualità dei processi tipici di ERP, CRM e asset management (letteralmente, "gestione delle risorse").

IoT: Il concetto rappresenta una possibile evoluzione dell'uso della rete internet: gli oggetti (le "cose") si rendono riconoscibili e acquisiscono intelligenza grazie al fatto di poter comunicare dati su se stessi e accedere ad informazioni aggregate da parte di altri. Tutti gli oggetti possono acquisire un ruolo attivo grazie al collegamento alla Rete. Per "cosa" o "oggetto" si può intendere più precisamente categorie quali: dispositivi, apparecchiature, impianti e sistemi, materiali e prodotti tangibili, opere e beni, macchine e attrezzature. Questi oggetti connessi che sono alla base dell'Internet delle cose si definiscono più propriamente smart objects (in italiano oggetti intelligenti) e si contraddistinguono per alcune proprietà o funzionalità. Le più importanti sono identificazione, connessione, localizzazione, capacità di elaborare dati e capacità di interagire con l'ambiente esterno.

On Premises: Il software on-premises (letteralmente "in sede, in locale, in ufficio"), in contrapposizione al software come servizio (o SaaS), si traduce in pratica nell'installazione ed esecuzione del software direttamente su macchina locale, sia essa aziendale che privata, intesa sia come singola postazione di lavoro che come server raggiungibile esclusivamente dall'interno della rete aziendale. L'approccio on-premises per la distribuzione/utilizzo del software è stato ritenuto la norma fino al 2005, data oltre la quale si è progressivamente ampliato l'utilizzo di software che esegue su computer remoti, da cui SaaS.

Cloud e SaaS (Software as a Service): In informatica con il termine inglese Cloud computing (in italiano nuvola informatica) si indica un paradigma di erogazione di servizi offerti on demand da un fornitore ad un cliente finale attraverso la rete Internet (come l'archiviazione, l'elaborazione o la trasmissione dati), a partire da un insieme di risorse preesistenti, configurabili e disponibili in remoto sotto forma di architettura distribuita. Le risorse non vengono pienamente configurate e messe in opera dal fornitore appositamente per l'utente, ma gli sono assegnate, rapidamente e convenientemente come servizio, grazie a procedure automatizzate, a partire da un insieme di risorse condivise con altri utenti lasciandogli parte dell'onere della configurazione. Quando l'utente rilascia la risorsa, essa viene similmente riconfigurata nello stato iniziale e rimessa a disposizione nel pool condiviso delle risorse, con altrettanta velocità ed economia per il fornitore.

Edge Computing: Serve a decentralizzare la nuvola, liberando certe applicazioni 'time-sensitive' dalla stretta dipendenza con i data center remoti, fornendo ad esse, come vedremo, la capacità, tramite l'uso di risorse di computing locali, di elaborare i dati direttamente sul campo.

AI (Artificial Intelligence): L'intelligenza artificiale (o IA, dalle iniziali delle due parole, in italiano) è una disciplina appartenente all'informatica che studia i fondamenti teorici, le metodologie e le tecniche che consentono la progettazione di sistemi hardware e sistemi di programmi software capaci di fornire all'elaboratore elettronico prestazioni che, a un osservatore comune,

sembrerebbero essere di pertinenza esclusiva dell'intelligenza umana. Può trovare espressione sia a livello centrale (Cloud On Premises) sia a livello distribuito on the Edge.

IoT Gateway: Un gateway (dall'inglese, portone, passaggio) è un dispositivo di rete che collega due reti informatiche di tipo diverso operando sia a livello di rete che ai livelli superiori, del modello ISO/OSI. Un IoT gateway è tipicamente un dispositivo più o meno dotato di capacità computazionale in grado di raccogliere dati da differenti protocolli di campo, attraverso interfacce diverse, in grado di elaborarli localmente, normalizzarli e renderli disponibili verso livelli superiori o esterni alla rete locale (ad esempio su Cloud). In particolare, un multi-service IoT gateway aggiunge diverse funzioni on the Edge grazie a framework applicativi che girano localmente sugli stessi. Tra queste funzioni l'astrazione del dispositivo stesso, l'interpretazione di svariati protocolli di campo, la gestione della connettività e della comunicazione, la gestione di flusso dati e analitiche, tool di configurazione e programmazione embedded, funzioni di amministrazione.

MQTT: MQ Telemetry Transport or Message Queue Telemetry Transport è un protocollo ISO standard (ISO/IEC PRF 20922) di messaggistica leggero di tipo publish-subscribe posizionato in cima al TCP/IP. È stato progettato per le situazioni in cui è richiesto un basso impatto e dove la banda è limitata. Il pattern publish-subscribe richiede un message broker. Il broker è responsabile della distribuzione dei messaggi ai client destinatari. Il protocollo è stato inventato nel 1999 da Andy Stanford-Clark di IBM, e Arlen Nipper, CTO di Eurotech Nord America e Cirrus Link Solutions.

API: In informatica, entro un programma, con Application Programming Interface (API) si indica un insieme di procedure (in genere raggruppate per strumenti specifici) atte all'espletamento di un dato compito; spesso tale termine designa le librerie software di un linguaggio di programmazione. Esistono vari design model per le API, sotto definiremo una REST API. Le interfacce intese per la massima velocità di esecuzione spesso consistono in una serie di funzioni, procedure, variabili e strutture dati. Una buona API fornisce una "scatola nera", cioè un livello di astrazione che evita al programmatore di sapere come funzionano le API ad un livello più basso. Questo permette di riprogettare o migliorare le funzioni all'interno dell'API senza cambiare il codice che si affida ad essa. La finalità è ottenere un'astrazione a più alto livello, di solito tra l'hardware e il programmatore o tra software a basso e quello ad alto livello semplificando così il lavoro di programmazione. Le API permettono infatti di evitare ai programmatori di riscrivere ogni volta tutte le funzioni necessarie al programma dal nulla, ovvero dal basso livello, rientrando quindi nel più vasto concetto di riuso di codice. Le API stesse rappresentano quindi un livello di astrazione intermedio: il software che fornisce una certa API è detto implementazione dell'API.

REST (API): Representational State Transfer (REST) è uno stile architetturale (di architettura software) per i sistemi distribuiti. L'espressione "Representational State Transfer" e il suo acronimo "REST" furono introdotti nel 2000 nella tesi di dottorato di Roy Fielding, uno dei principali autori delle specifiche dell'Hypertext Transfer Protocol (HTTP), e vennero rapidamente adottati dalla comunità di sviluppatori su Internet. Il termine REST rappresenta un sistema di trasmissione di dati su HTTP senza ulteriori livelli (quali ad esempio SOAP). I sistemi REST non prevedono il concetto di sessione (sono, come approfondito successivamente, stateless). L'architettura REST si basa su HTTP; il funzionamento prevede una struttura degli URL ben definita (atta a identificare univocamente una risorsa o un insieme di risorse) e l'utilizzo dei verbi HTTP specifici per il recupero di informazioni (GET), per la modifica (POST, PUT, PATCH, DELETE) e per altri scopi (OPTIONS, ecc.).

Digital Twin: Tra le tante definizioni che seguono quella già presentata in questo libro, un'interessante nuova dinamica è stata data da Robert Plana, Innovation & Ecosystem Director di GE Digital, società del gruppo General Electric che sviluppa soluzioni per l'IoT, che così la descrive: «Il digital twin è una sorta di modello in vivo di un impianto o di una linea di produzione, realizzato dall'incrocio tra i dati reali di funzionamento e i disegni cad e digitali serviti per la progettazione. Il digital twin consente di costruire una copia virtuale dell'impianto reale, ma anche di una singola macchina, in grado di replicare in tutto e per tutto il funzionamento reale o di verificarne tutte le possibili alternative». Di immediata estensione a qualsiasi altro contesto, quello del building ad esempio.

BIM: Il Building Information Modeling (acronimo: BIM, in italiano: Modellizzazione delle Informazioni di Costruzione) indica un metodo per l'ottimizzazione della pianificazione, realizzazione e gestione di costruzioni tramite aiuto di un software. Tramite esso tutti i dati rilevanti di una costruzione possono essere raccolti, combinati e collegati digitalmente. La costruzione virtuale è visualizzabile inoltre come un modello geometrico tridimensionale. Il Building Information Modelling viene utilizzato sia nel settore edile per la progettazione e costruzione (architettura, ingegneria, impianti tecnici) come anche nel facility management.

Industria 4.0: Il termine Industria 4.0 indica una tendenza dell'automazione industriale che integra alcune nuove tecnologie produttive per migliorare le condizioni di lavoro, creare nuovi modelli di business e aumentare la produttività e la qualità produttiva degli impianti. Industria 4.0, prende il nome dall'iniziativa europea Industry 4.0, a sua volta ispirata ad un progetto voluto dal governo tedesco. Nello specifico la paternità del termine tedesco **Industrie 4.0** viene attribuita a Henning Kagermann, Wolf-Dieter Lukas e Wolfgang Wahlster che lo impiegarono per la prima volta in una comunicazione, tenuta alla Fiera di Hannover del 2011, in cui preannunciarono lo "Zukunftsprojekt Industrie 4.0". Concretizzato alla fine del 2013, il progetto per l'industria del futuro "Industrie 4.0" prevedeva investimenti su infrastrutture, scuole, sistemi energetici, enti di ricerca e aziende per ammodernare il sistema produttivo tedesco e riportare la manifattura tedesca ai vertici mondiali, rendendola competitiva a livello globale.

Servitization: La servitizzazione è generalmente riconosciuta come un processo di trasformazione del modello di business da una prospettiva prodotto-centrica a una cliente-centrica, in cui il servizio rappresenta la componente fondamentale.

API Economy: L'economia delle API – uno scambio commerciale di funzioni di business, capacità o competenze sotto forma di servizi esposti nelle API – rappresenta la forza motrice di gran parte dell'evoluzione digitale di molti settori, permettendo di trasformare le organizzazioni, creare nuovi ecosistemi e monetizzare i principali asset, servizi e prodotti.

App Economy: ovvero dell'insieme di attività economiche che derivano dal grande successo delle applicazioni che utilizzano il Cloud, ed in particolare delle applicazioni mobili. La App Economy non solo comprende la vendita delle applicazioni, ma include anche la pubblicità, la vendita dei dispositivi su cui vengono eseguite le App ed in generale tutte le fonti di redditività collegate in modo diretto o indiretto al Cloud.

Cosa significa e le opportunità dell'IoT

Nell'ormai lontano 1990, durante la INTEROP Internet Networking Conference, la star dello show fu un tostapane. Questo è, secondo gli storici della Rete, il momento preciso della nascita dell'Internet of Things (IoT): un umile esordio che segna la partenza della profonda trasformazione che stiamo vivendo. Per la prima volta dispositivi fisici, reti e protocolli si coordinano, creando un continuum architetturale ed un tostapane si affaccia su Internet per comunicare il proprio stato, essere monitorato e controllato. Se in quel momento l'intervento umano era ancora richiesto per inserire il pane, già dall'edizione successiva anche questo elemento veniva rimosso grazie ad un automatismo, completando così una catena in cui le macchine iniziavano a cooperare per produrre in modo trasparente un risultato fruibile.

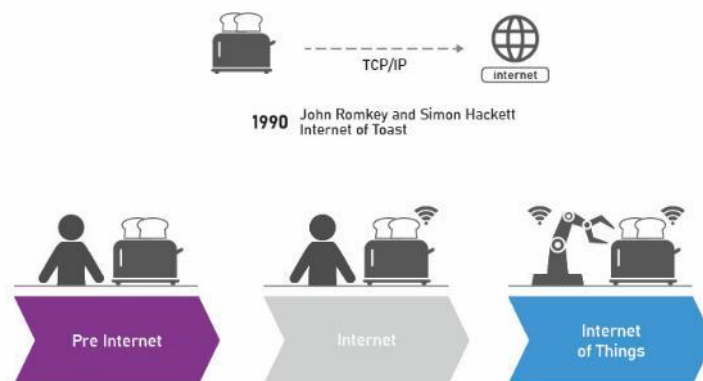


Figura 1: Il primo tostapane connesso

Perché ora si parla di IoT: il contesto tecnologico globale

Evoluzione tecnologica, disponibilità di sensori intelligenti e connessi, connettività con tecnologie a basso costo

Se la comparsa del primo esempio di IoT può essere datata 1990¹, è a partire dagli anni 2000 che si assiste alla crescita esponenziale delle connessioni cellulari, con un susseguirsi di generazioni tecnologiche sempre più orientate al trasferimento del dato. Dietro a questa grande crescita c'è il progresso tecnologico che riduce costi e dimensioni dei calcolatori e viene ben descritto dalla cosiddetta legge di Moore². Chi si accorse per primo del fenomeno, fino ad oggi inarrestabile, della deflazione dei costi del transistor - mattone fondamentale di costruzione di qualsiasi dispositivo elettronico digitale – fu, negli anni 60, Gordon Moore, uno dei fondatori di Intel e uno dei padri del transistor. La sua legge di scala dice che circa ogni due anni le prestazioni raddoppiano a parità di costo o che a parità di prestazioni il costo si dimezza. Dopo 60 anni di incessante applicazione di

¹ "Toast of the IoT: The 1990 Interop Internet Toaster" – John Romkey – IEEE

² https://en.wikipedia.org/wiki/Moore%27s_law

questa legge, il risultato evidente è la riduzione esponenziale dei costi dei prodotti elettronici e la altrettanto esplosiva crescita della densità della capacità di processare, memorizzare e trasmettere le informazioni. Questa combinazione di fattori ci proietta nella nuova era dell'Internet delle "Cose" (o IoT, ovvero Internet of Things), dove per "Cosa" si intende qualsiasi oggetto fisico che contenga in sé una tecnologia per comunicare e rilevare o interagire con i propri stati interni o con l'ambiente esterno³.

Della legge di Moore hanno beneficiato in larghissima misura le infrastrutture di comunicazione telefoniche e le nuove reti cellulari. La connettività cellulare infatti (e più in generale wireless) è un pilastro dell'IoT, dal momento che consente di raggiungere le "Cose", ovunque esse siano, ad una frazione del costo richiesto dalle tradizionali reti cablate.

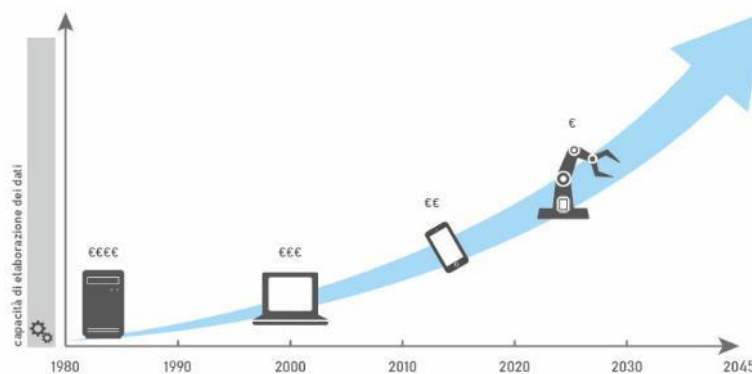


Figura 2: La legge di Moore

Man mano che le reti cellulari raggiungono un numero sempre maggiore di utenti, aumenta anche la copertura territoriale del segnale. Ad esempio secondo i dati della World Bank⁴, nel 2015 ogni 100 persone si registravano ben 101.5 sottoscrizioni per dispositivi mobili cellulari. Allo stesso modo aumenta esponenzialmente anche il traffico dati: secondo il Cisco Visual Networking Index⁵ del 2016, nei precedenti cinque anni la quantità di dati dovuti a dispositivi mobili è cresciuta di ben 18 volte. Sempre secondo questo studio, il Medio Oriente, l'Africa, la regione Asia-Pacifico e l'America Latina avrebbero esibito i più alti tassi di aumento delle sottoscrizioni. Le due conseguenze dirette di questa espansione sono da un lato una copertura territoriale assolutamente capillare a livello globale, e dall'altro la necessità per le Telecom ed i Carrier di identificare nuove opportunità di crescita nei mercati saturi (Europa, Stati Uniti, solo per citare due esempi).

³ <https://www.gartner.com/it-glossary/internet-of-things>

⁴ <https://data.worldbank.org/indicator/IT.CEL.SETS.P2?end=2016&start=1981>

⁵ <https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/mobile-white-paper-c11-520862.html>

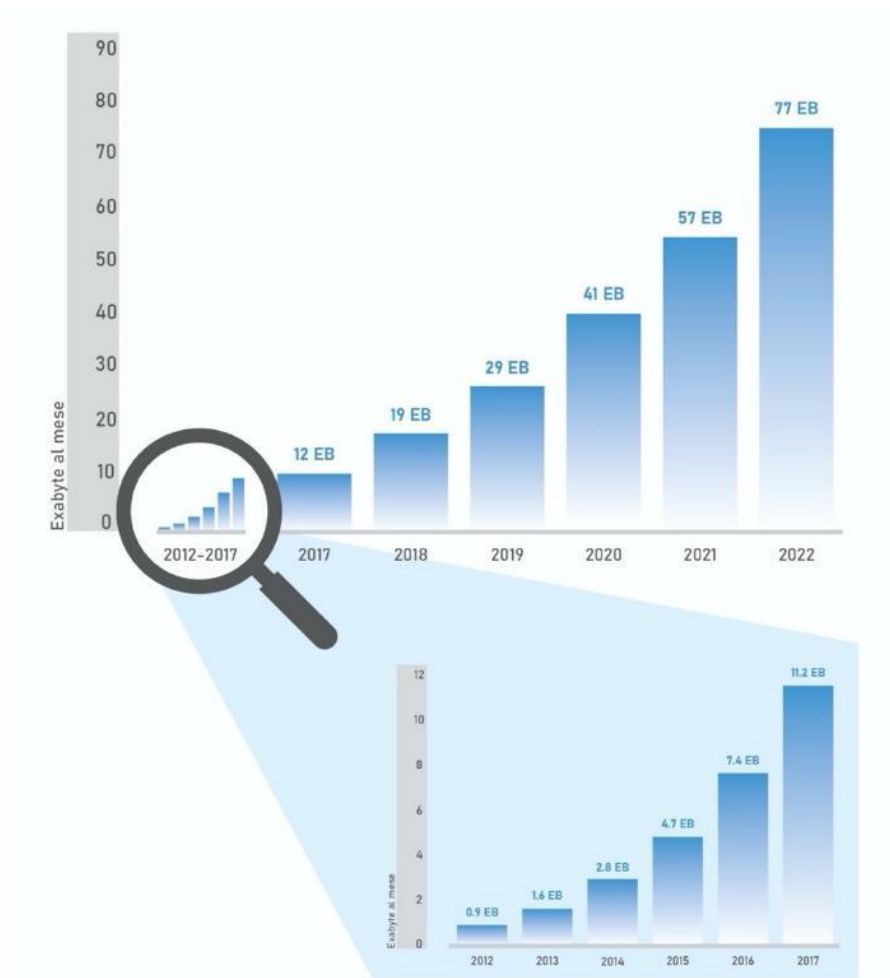


Figura 3: Cisco Visual Networking Index 2017

Questo secondo aspetto in particolare è molto importante, dal momento che il numero delle “Cose” è potenzialmente ordini di grandezza maggiore del numero delle persone; da qui la motivazione molto forte per le Telecom ed i Carrier a favorire la diffusione dell’IoT anche mediante l’introduzione di tecnologie mirate. Ne sono un esempio M1 e NB-IoT, due varianti molto specializzate (“Narrow Band”) di tecnologia cellulare LTE che estendono il 4G nel dominio delle applicazioni in cui la durata della batteria deve essere dell’ordine dell’anno e nelle quali la trasmissione dei dati è sporadica (come nel caso degli Smart Meter).

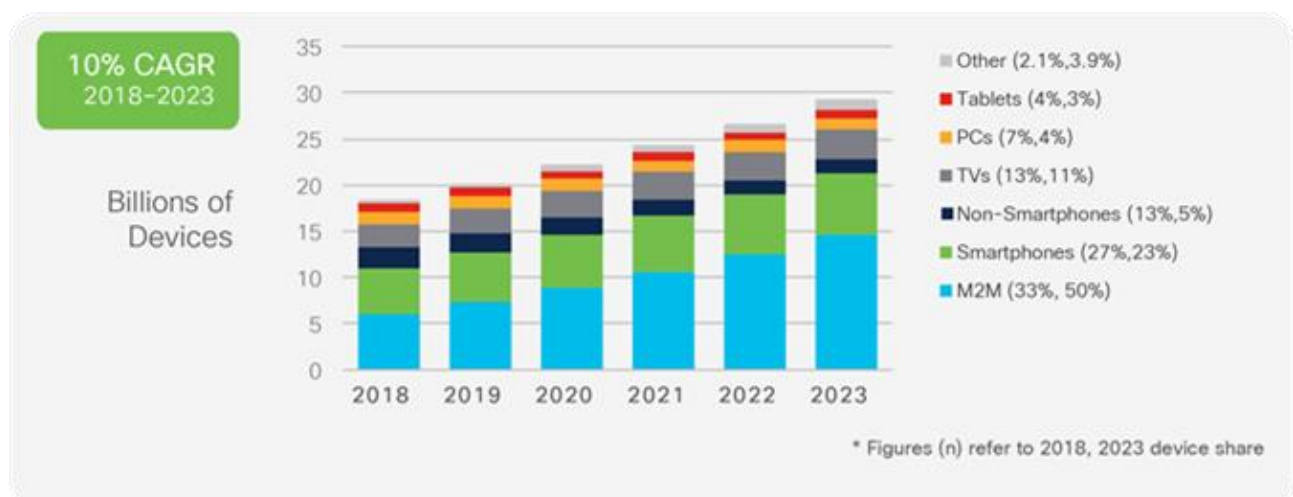
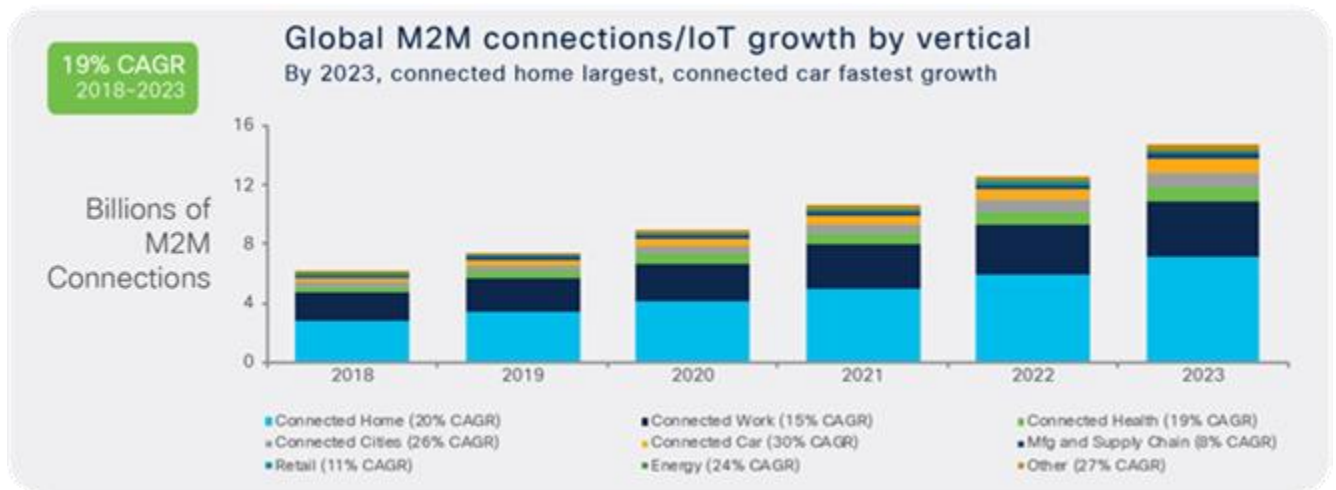


Figura 4: Source: Cisco Annual Internet Report, 2018–2023



Source: Cisco Annual Internet Report, 2018–2023

Figura 5: Crescita connessioni M2M per segmenti applicativi

Nel 2019, sempre secondo il Rapporto Cisco 2020, le reti cellulari 4G hanno superato per diffusione quelle precedenti a basse performance in termini di connettività. Nel 2023 si stimano 6 miliardi di dispositivi 4G rispetto ai 3,7 miliardi del 2018, mentre i dispositivi 5G passeranno dai 13 milioni del 2019 agli 1,4 miliardi nel 2023.

Le reti cellulari 4G si stanno evolvendo per offrire servizi dedicati all'IoT (e del tutto distinti da quelli per la fruizione del cliente tradizionale) anche per contrastare tecnologie emergenti che vanno collettivamente sotto il nome di LPWAN (Low-Power, Wide Area Network).

Con il termine LPWAN si intendono sistemi radio diversi dalle varianti Narrow Band del 4G LTE, ma che sono indirizzati allo stesso fine, ovvero consentire l'introduzione della comunicazione wireless nelle "Cose", senza per questo incrementarne in modo sensibile il costo, garantendo un grande raggio d'azione e una lunga durata operativa. Alcuni esempi di sistemi LPWAN sono: LoRaWAN, Weightless (entrambi emanati da consorzi), Sigfox, RPMA e SymphonyLink (proprietary).

La tecnologia LPWAN, per quanto adatta ad oggetti a limitata intelligenza dove non sia necessario garantire aggiornamenti remoti (quali gli "smart meters"), trova una sua collocazione soprattutto nelle architetture proprietarie Sigfox. Nel momento in cui il caso d'uso richieda anche un'interazione più spinta con il campo, giustificata ad esempio da messaggi dal Cloud alla periferia per device management, queste architetture perdono di efficacia e vengono a queste preferite le cosiddette LPW/PAN (Low-Power Wide Peripheral Area Network).

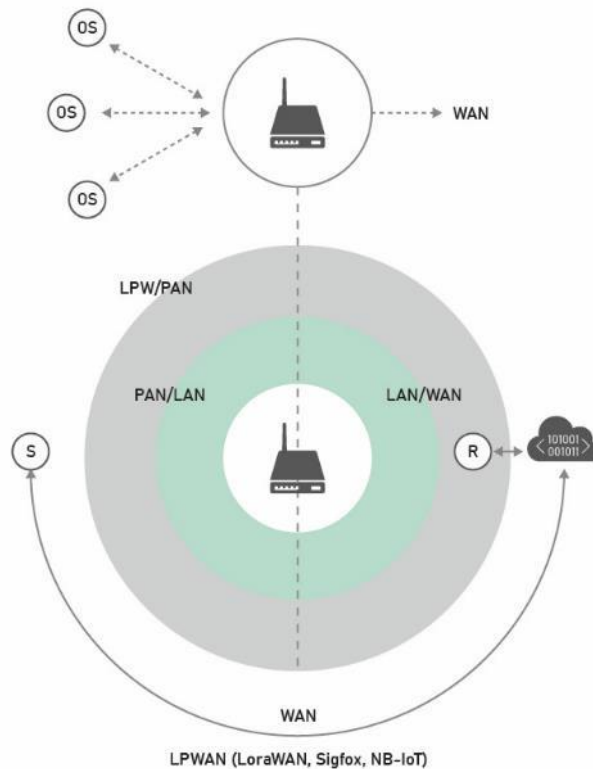


Figura 6: LPW/PAN (Low Power Wide Peripheral Area Network)

In questo scenario, più affine allo standard LoraWAN, continuano a coesistere sensori ed oggetti con intelligenza limitata diventando però lo strato di campo periferico (“field”) di IoT gateway ed Edge computer, gli oggetti a maggior intelligenza che si occupano di fare aggregazioni, correlazioni e portare logica ed aggiornamenti on the Edge. Sono quindi i gateway a comunicare verso il Cloud attraverso LAN/WAN le metriche trasparentemente raccolte dal campo ed i risultati di eventuali analitiche eseguite a livello Edge, oltre che a prendere in carico le operazioni di downlink per aggiornamento remoto.

Questo elenco non sarebbe tuttavia completo se non si menzionassero le reti 5G, che hanno le applicazioni IoT nel proprio DNA. Queste reti, interoperabili con quelle 4G e attive anche su nuove bande (frequenze maggiori di 6GHz), offriranno prestazioni molto superiori a quelle correnti, con una velocità anche cento volte maggiore, una latenza di rete fino a cinque volte inferiore e una capacità di traffico dati potenzialmente mille volte più grande. In aggiunta a queste caratteristiche, alcune nuove capacità permetteranno di introdurre innovazioni molto rilevanti nell’ambito dell’IoT: una riduzione dei consumi che permetterà 10 anni o più di funzionamento per i dispositivi alimentati a batteria, comunicazione praticamente istantanea (in virtù della bassa latenza), partizionamento del network al fine di adattare localmente velocità, capacità e latenza della rete in funzione di casi d’uso specifici.

Storia di una evoluzione: da M2M a IoT

Da Machine to Machine a IoT, evoluzione ed estensione, limiti del M2M e integrazione in un sistema IoT

I computer, quelli che conosciamo noi, da quando sono stati inventati sono stati sempre interconnessi con il mondo esterno, anche perché un computer senza un input ed un output non ha senso di esistere nel nostro mondo. Le interconnessioni da locali hanno raggiunto distanze sempre maggiori e una più capillare diffusione man mano che le reti di telecomunicazione sono progredite. Quando i calcolatori, grazie alla miniaturizzazione e all'abbattimento dei costi, sono entrati nell'automazione delle macchine, si è coniato il termine Machine to Machine (M2M) per descrivere la comunicazione tra computer. Con il termine M2M (Machine to Machine) si descrive quindi un'architettura in cui le "Cose", in questo caso macchinari, sono in grado di dialogare tra loro. Ciò potrebbe indurre a pensare che IoT ed M2M siano due termini intercambiabili, quando invece rappresentano due concetti distinti, di cui al più si potrebbe pensare all'M2M come precursore dell'IoT.

Le principali differenze tra IoT ed M2M sono: la pervasività ("Cose"/macchine), il contesto (connesso/isolato), la tecnologia di rete (Internet/altre), le competenze coinvolte (tecnologie informatiche/tecnologie dei dispositivi), la scalabilità (semplice/complessa), l'approccio (standard/proprietario), il tempo di reazione (quasi real-time/batch) e la garanzia di consegna del dato (garantita/best effort).

Il concetto M2M risale ai primi anni '70, quando Theodore Paraskevakos⁶ combinò telefonia e computazione in un brevetto per un sistema di identificazione della chiamata ("Caller ID"); seguirono rapidamente molti altri dispositivi che pur essendo destinati ad applicazioni molto diverse, come ad esempio lo "Automatic Meter Reading", condividevano gli stessi principi fondamentali, ovvero la presenza simultanea di una qualche capacità di calcolo unita alla comunicazione.

Il termine IoT fu coniato nel 1999 da Kevin Ashton⁷, che a sua volta era stato influenzato dal libro "When Things Start to Think" di Neil Gershenfed⁸.

Ashton, che allora lavorava presso un'importante azienda di cosmetici, diede una presentazione il cui titolo era "Internet of Things"⁹. L'oggetto della presentazione era una possibile soluzione al problema della tracciatura dei prodotti. Fino a quel tempo, il sistema allo stato dell'arte consisteva nell'impiego di codici a barre, con i quali venivano "marcati" i passaggi da un punto all'altro. Il problema tuttavia era solo mitigato: il codice a barre poteva al massimo confermare la presenza del prodotto nel negozio, ma non la sua posizione, quindi non c'era modo di sapere se si trovasse nel magazzino o sullo scaffale. Ashton illustrò una strategia che invertiva il punto di vista: dotando ogni prodotto di un RFID (Radio Frequency Identification) sarebbero stati i prodotti stessi a dichiarare autonomamente, ed in ogni istante, la loro posizione. Il caso pratico che ispirò questa nuova metodologia fu un particolare tipo di rossetto, che pur abbondando nei magazzini, era sempre esaurito sullo scaffale. Con l'approccio "IoT", lo scaffale ed il rossetto avrebbero potuto comunicare, così come il rossetto ed il magazzino e così via.

Volendo sintetizzare in un solo concetto la differenza tra M2M ed IoT bisogna focalizzare l'attenzione sul dato e la sua accessibilità. L'M2M predata l'IoT e si colloca in un periodo storico in

⁶ https://en.wikipedia.org/wiki/Machine_to_machine

⁷ <https://www.smithsonianmag.com/innovation/kevin-ashton-describes-the-internet-of-things-180953749/>

⁸ <https://dl.acm.org/citation.cfm?id=519271>

⁹ http://ethw.org/Kevin_Ashton

cui le risorse informatiche (comunicazione, memoria, capacità di calcolo) erano infinitamente più limitate e molto più costose di quanto lo siano oggi. Ciò ha fatto sì che il dato venisse trattato “ad hoc”, con l’obiettivo di ridurne la quantità. In pratica, non potendo trasferire il contesto (ovvero tutta l’informazione accessoria), ma solo l’informazione strettamente essenziale, nell’M2M era l’applicazione a farsi carico della ricostruzione del contesto. Ad esempio, in una applicazione in cui veniva richiesto il monitoraggio della temperatura, tipicamente veniva riportato solo questo valore. Tutto il contesto (ad esempio posizione geografica) veniva scartato perché l’applicazione che consumava il dato di temperatura veniva scritta assumendo “a priori” che il dato fosse originato in un certo posto. L’estrema efficienza di questa metodologia aveva l’effetto collaterale di creare dei “Data Silos”, ovvero dei serbatoi di dati “decontestualizzati” o poveri di informazione relativa al contesto; ciò comportava la difficoltà di riutilizzare questi dati, poveri di contesto, in altre applicazioni (o in applicazioni scritte in un tempo successivo) perché era solitamente molto difficile estrarre dall’applicazione i presupposti (condizioni al contorno) e perché i dati stessi non offrivano tutto il dettaglio richiesto.

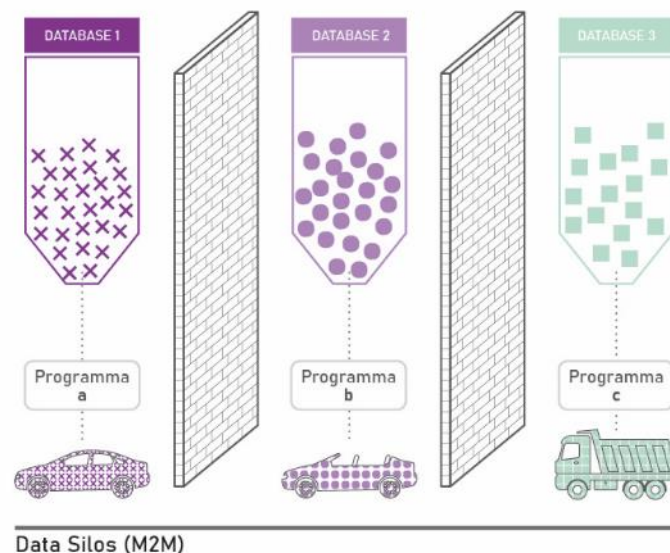


Figura 7: Data Silos

Con l’IoT la prospettiva cambia, anche grazie al progresso tecnologico che, nel frattempo, ha reso non solo possibili ma anche economici la memorizzazione e il processamento di grandi quantità di dati. Poiché oramai risultano abbattute le barriere che impedivano di arricchire il dato con le informazioni relative al contesto, diventa oggi possibile memorizzare tutto il dettaglio necessario per una sua descrizione esaustiva, dunque con valore permanente del dato stesso e che va al di là della singola applicazione che lo userà. In aggiunta a questo, nell’IoT il concetto di database si rende molto più elastico di quanto accadeva nell’M2M, dove il dato era necessariamente molto scarno per consentirne una efficiente manipolazione.

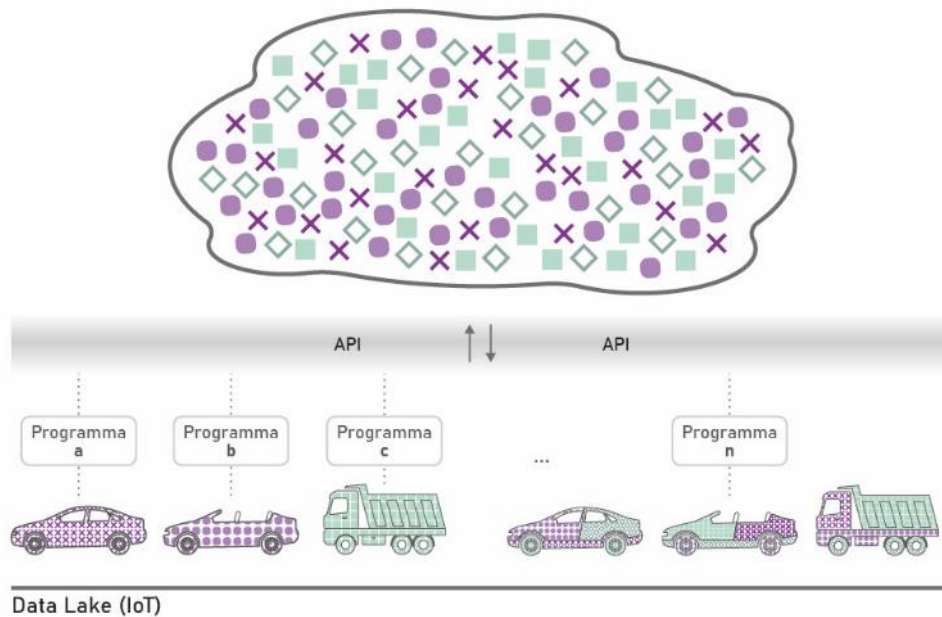


Figura 8: Data Lake

Di fatto, si sostituisce il concetto di “Data Silos” con quello di “Data Lake”, in cui il dato diventa interoperabile e privo di uno scopo aprioristico.

Tutto ciò viene reso possibile da nuovi framework che racchiudono in uno stesso strumento lo storage distribuito e l’elaborazione del set di dati in esso contenuto. Un esempio è Apache Hadoop¹⁰, un ambiente di lavoro che mette assieme un File System distribuito (HDFS – Hadoop Distributed File System) con MapReduce¹¹, ovvero un modello di programmazione altamente scalabile che consente di processare e generare dataset di grandi dimensioni.

A differenza di quanto accadeva normalmente nell’M2M, nell’IoT il dato diventa “ricco” ed “agnostico”, la sua manipolazione ed il trasferimento tra applicazioni estremamente agevole.

Anatomia di una soluzione IoT

Descrizione dell’IoT, definizione, componenti principali e loro funzionamento

IoT è un termine tecnico che definisce con efficacia il concetto che rappresenta: un sistema attraverso il quale le “Cose” possono comunicare con noi e tra loro, in modo analogo a quanto già fanno le persone attraverso Internet.

Da questo scenario emergono chiaramente gli elementi costitutivi e fondanti di una architettura IoT: ovvero (a) le “Cose”, (b) quello che serve alle “Cose” per connettersi alla Rete Internet e quindi trasportare i dati nel Cloud dove possono venire inviati agli utilizzatori o memorizzati, (c) la visualizzazione e interpretazione dei dati provenienti dalle “Cose” così da poter permettere l’iterazione tra di esse e con esse.

¹⁰ <http://hadoop.apache.org/>

¹¹ https://hadoop.apache.org/docs/r1.2.1/mapred_tutorial.html

Il primo concetto, la “Cosa”, è un sottosistema del mondo fisico che si concretizza in innumerevoli dispositivi con vari livelli di complessità: da cose semplicissime come il sensore che registra una temperatura o il motore (attuatore) che apre un cancello, fino a sistemi molto complessi come una casa, un treno o un impianto industriale. Per poter trovare una sua collocazione all’interno dell’IoT, la “Cosa” deve necessariamente essere dotata di un sistema di comunicazione che la metta in grado di inviare dati nella rete Internet, il secondo elemento costruttivo dell’IoT. Le “Cose” che oggi ci circondano possono presentarsi, per quanto riguarda la connessione alla rete, in più modalità che in primissima approssimazione possiamo dividere in quattro macro-categorie:

- 1 - “Cosa” non connessa alla rete e/o “Cosa” non elettronica
- 2 - “Cosa” connessa solo ad una rete locale
- 3 - “Cosa” connessa ad una rete che non supporta il protocollo di Internet
- 4 - “Cosa” connessa ad Internet

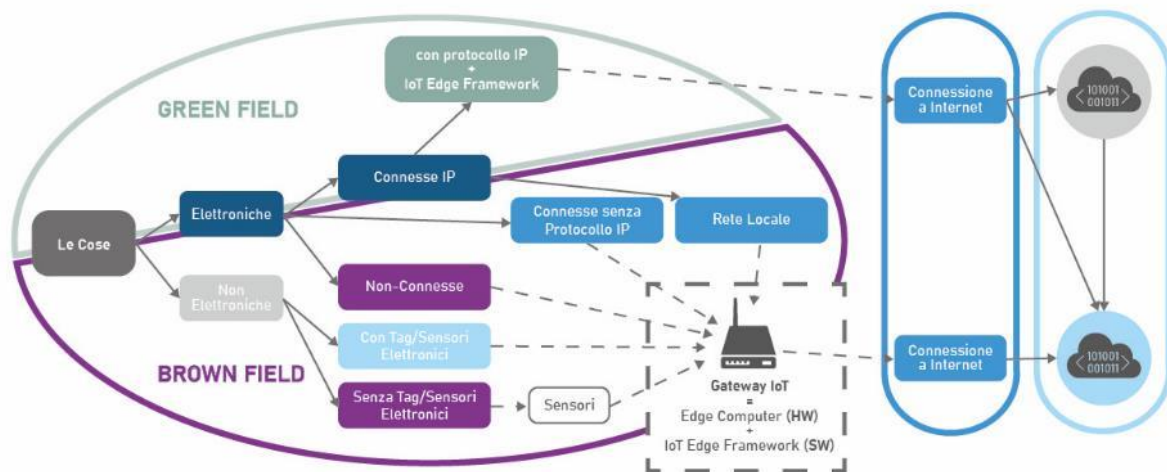


Figura 9: “Cose” connesse e non nel green e brown field

Da questa osservazione sulle “Cose” emerge l’importanza del secondo elemento costruttivo dell’IoT e che riguarda appunto il collegamento della “Cosa” alla rete Internet. La connessione ad Internet va però considerata come condizione necessaria ma non sufficiente per poter parlare di IoT. L’IoT va oltre il concetto di “Cosa” connessa ad Internet e riguarda principalmente l’interoperabilità tra “Cose” eterogenee attraverso i dati che da esse provengono. Se non si è in grado di poter sfruttare i dati prodotti in modo nativo dalle “Cose” per creare nuovi significati e nuove applicazioni non si è in presenza di una implementazione IoT, bensì di una implementazione M2M proprietaria in cui i dati provenienti dalle “Cose” rimangono isolati dentro una ben predeterminata applicazione e non sono fruibili per poter generare altro valore all’infuori della applicazione nativa (come introdotto nel precedente paragrafo e rappresentato nel Data Silos di figura 5).

All’interno delle macro-categorie summenzionate è possibile individuare ulteriori livelli di classificazione, che qualificano ulteriormente delle caratteristiche relative a vari aspetti della “Cosa” e che risultano essere molto utili per collocare la “Cosa” in un contesto applicativo; alcune caratteristiche spesso prese in considerazione sono:

1. l'autonomia: tipo di batteria, possibilità di ricarica da fonte rinnovabile, durata, etc.
2. i tipi di connessione: locali (Wi-Fi o BLE), geografiche (Sigfox, LoRa, etc.) o di entrambi i tipi
3. la frequenza di invio dati sul Cloud: quartoraria, oraria, giornaliera, etc.
4. la disponibilità dei dati per applicazioni di terze parti.

Dopo le “Cose”, l'altro pilastro fondamentale per l'IoT è la Rete, che presenta tanto aspetti fisici (il mezzo di comunicazione) che logici (la topologia ed i protocolli). Analizzando per prima la parte fisica della Rete si vede che è costituita da due componenti: il mezzo (cavo di rame, fibra ottica od il campo elettromagnetico nel caso delle tecnologie wireless e cellulari) ed il transceiver, ovvero il dispositivo che trasforma i dati digitali in segnali elettrici, ottici o radio e viceversa.

Le componenti logiche della Rete sono ciò che la caratterizza maggiormente da un punto di vista funzionale; sono inoltre spesso strettamente correlate.

La topologia è il componente che si pone a cavallo tra la parte fisica e quella logica: corrisponde allo schema dei collegamenti che permettono ai dati di andare da un punto ad un altro; tra le topologie più comuni ci sono quella diretta punto-punto, la stella con un aggregatore centrale e la “mesh”, in cui ogni elemento è connesso con i suoi vicini.

I dati, per potersi muovere lungo il mezzo fisico, attraversandone i rami organizzati in una topologia, devono seguire certe regole che consentono di interpretare e gestire alcuni parametri essenziali, quali l'indirizzo di destinazione, l'integrità dell'informazione, e così via.

Il secondo componente logico è il *protocollo*, ovvero l'insieme di regole e procedure che rendono possibile la comunicazione tra computer, regolamentando le transazioni e dando struttura ai dati che vengono scambiati.

Una caratteristica importante dei protocolli è che normalmente sono finalizzati ad uno scopo molto specifico e per questo motivo è comune che i protocolli siano stratificati uno sull'altro, o addirittura incapsulati uno nell'altro. È possibile classificare i protocolli in funzione del livello (o strato) a cui appartengono: Infrastruttura, Identificazione, Comunicazione e Trasporto, Scoperta, Dato, Manutenzione, Semantica, Multi-Livello, Sicurezza, Applicazione.

Lo strato fondamentale su cui tutti gli altri appoggiano è quello della Infrastruttura, che normalmente è lo stesso di Internet (IPv4/IPv6); per questo motivo tecnico l'IoT è definita come Internet of Things¹²; in alcuni casi i protocolli impiegati sono quelli diffusamente utilizzati dalla maggior parte delle applicazioni che sfruttano la rete, mentre in altri (vedi ad esempio MQTT e CoAP) si tratta di protocolli usati prevalentemente da applicazioni IoT.

L'altro importante elemento della connessione della “Cosa” è il suo punto di “aggancio” alla Rete, che è detto *interfaccia* e che come tale dipende dal tipo di “Cosa”; l'interfaccia deve rispondere tanto ai requisiti fisici dell'ambiente in cui la “Cosa” è collocata, quanto a quelli informatici della Rete. La grande varietà di punti di aggancio ha dato vita al concetto di *IoT-Gateway* ovvero di un oggetto che fa da porta di accesso per la “Cosa” nella rete IP, facendo da “traduttore” che digitalizza gli stati interni della “Cosa” (o i valori che la “Cosa” registra dal mondo esterno), per poi inviarli alla rete.

¹² <https://www.postscapes.com/internet-of-things-protocols/>

Il valore dell'IoT-Gateway risiede nell'essere lo strumento "abilitatore" dell'IoT, come risulta evidente se lo riferiamo alle macro-categorie con cui vengono classificate le "Cose".

Se prendiamo le "Cose" di tipo 1 (non connesse alla rete e/o non elettroniche) va da sé che, per introdurle in una architettura IoT, a queste vada abbinata un'unità di calcolo che deve rispondere ad alcuni requisiti:

- deve essere dotata di apposite interfacce attraverso le quali vengono letti gli stati della "Cosa";
- deve poter trasformare poi gli stati della "Cosa" nelle loro rappresentazioni digitali, ovvero in dati che verranno poi immessi nella Rete;
- deve essere collegata alla Rete;
- deve poter gestire uno o più protocolli.

Di fatto, l'insieme di tali requisiti è un sottoinsieme delle caratteristiche offerte da un IoT Gateway.

Per le "Cose" di tipo 2 (connesse solo ad una rete locale), pur essendo queste dotate di unità di calcolo e di interfacce, sono di fatto confinate in contesti molto specifici. In questo caso i problemi sono principalmente due:

- la mancanza di un paradigma comune nella interpretazione e gestione del dato;
- l'enorme varietà di interfacce: da quelle standard e popolari come la seriale RS-485, a quelle standard ma specializzate (KNX, usato nella Domotica/Building Automation), fino ad arrivare al caso estremo, ma comune, delle interfacce proprietarie.

L'elemento architetturale che consente anche in questo caso di armonizzare la pletora di interfacce di campo è sempre l'IoT Gateway. È proprio nell'IoT Gateway che si compie la fusione tra il mondo fisico dei sensori e delle macchine (detto anche mondo OT, da "Operational Technology") e quello dei dati, ovvero dell'"Information Technology" (IT), due ambiti che prima dell'avvento dell'IoT erano tradizionalmente distinti e difficilmente interoperabili.

Anche per le "Cose" di tipo 3 (connesse ad una rete che non supporta il protocollo di Internet) sono richiesti, nella maggior parte dei casi, degli IoT Gateway o in loro assenza, per far comunicare queste "Cose" con altre "Cose" attraverso il Cloud, dovranno essere messe a disposizione delle connessioni logiche Cloud-to-Cloud.

Analogo discorso può essere fatto per le "Cose" di tipo 4 (connesse ad Internet): qualora non fosse disponibile un connettore Cloud-to Cloud bisognerà dotare anche queste "Cose" di un IoT Gateway.

Semplificando al massimo, l'IoT Gateway presenta da un lato una o più interfacce di campo collegate alle "Cose" e dall'altro almeno un canale di comunicazione verso la Rete Internet. Il Gateway deve come minimo offrire il servizio di trasferimento del dato in maniera bidirezionale tra Internet ed il campo, ma naturalmente esistono Gateway che aggiungono capacità più sofisticate ("multi-service" IoT Gateway), come ad esempio i servizi di aggregazione e filtraggio dei dati, programmi locali che agiscono istantaneamente all'accadere di alcuni eventi, ed altre funzioni di monitoraggio e gestione delle "Cose".



Figura 10: Embedded Computer e Gateway

Naturalmente, il Gateway può esistere come dispositivo a sé stante, oppure come elemento integrato all'interno di una "Cosa"; a loro volta i Gateway (integrati o meno) possono essere inseriti all'interno di una struttura che potremmo definire per certi aspetti gerarchica, ma che in realtà è più a calcolo distribuito; in questo caso si parla di "Fog Computing". Secondo il paradigma del "Fog Computing" il Gateway non è più connesso direttamente ad Internet, ma ne fa parte come ramo periferico agganciato ad un apparato più potente detto Edge Computer, ovvero una specie di super-gateway che aggrega più gruppi di Gateway e di "Cose". Per esempio, una fabbrica potrebbe avere al suo interno numerosi IoT Gateway più o meno sofisticati che afferiscono ad un Edge Computer anch'esso locale, il quale diventa il Gateway della fabbrica e, come tale, astrae tutta la fabbrica in una sua rappresentazione digitalizzata alla rete Internet.

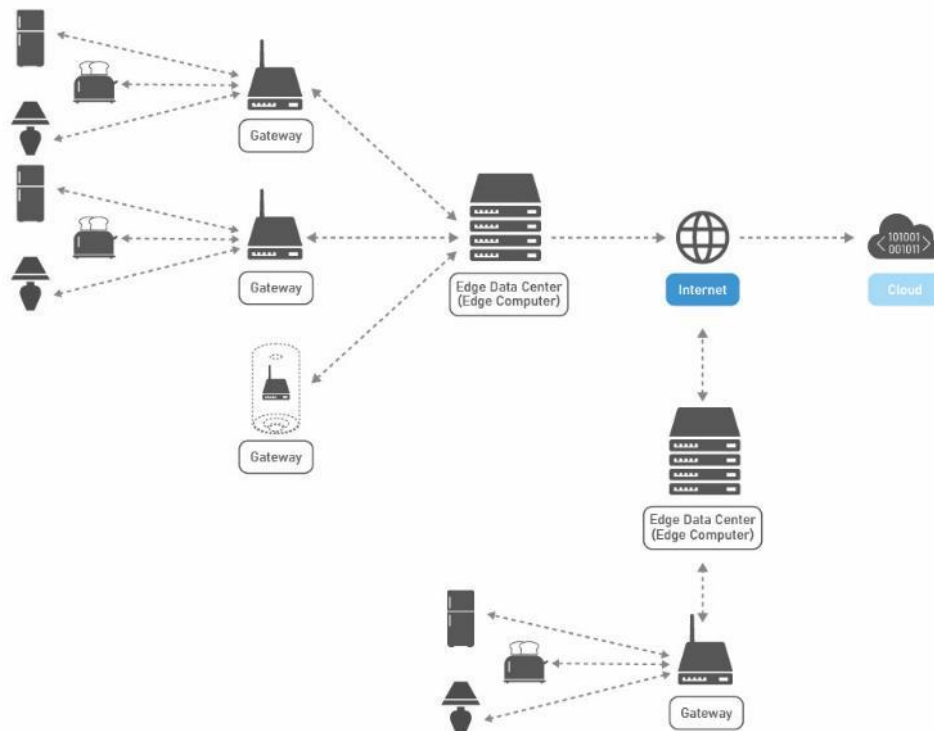


Figura 11: Gateway ed Edge Computer

Grazie alla mediazione dell'Edge Computer, il "Fog Computing" consente di dare una risposta efficiente alle richieste di resilienza, di tempi di intervento Near-Real-Time e di elaborazione (per complessità o quantità di dati) che sono critici in molte applicazioni.

L'Edge Computer è, in questo senso, una estensione del Data Center e ne possiede le qualità fondamentali (potenza di calcolo, ampia memoria), aggiungendo spesso caratteristiche di robustezza fisica che ne abilitano l'uso anche in contesti gravosi, come le fabbriche.

Grazie alle sue capacità, l'Edge Computer consente di effettuare direttamente sul campo, o in sua prossimità, una serie di interventi sul flusso di dati provenienti dai Gateway che vi afferiscono. Ad esempio, l'Edge Computer può memorizzare tutti i dati ed operare su di essi mediante algoritmi sofisticati e con l'obiettivo di integrare le diverse fonti e di fornire una interpretazione del contesto. Questo approccio produce numerosi benefici: la prossimità (spesso il collegamento diretto) dell'Edge Computer alle fonti di dati permette di avere un comportamento deterministico e Near-Real-Time; la capacità di memorizzare ed elaborare tutti i dati consente un risparmio estremamente significativo nella quantità di informazione trasmessa verso la Rete (con conseguente abbattimento dei costi operativi). Inoltre, dal momento che l'Edge Computer è una estensione del Data Center, la sua presenza in una architettura offre garanzie di continuità operativa, ovvero Quality of Service (QoS), anche nel caso la connettività verso la Rete venga meno.

L'ultimo pilastro dell'IoT è costituito dal layer di visualizzazione e attuazione, ovvero da applicazioni e programmi (anche facenti uso di elementi di Intelligenza Artificiale) che consentono agli umani o ai computer di prendere delle decisioni in base ai dati ricevuti dalle "Cose". Tutto questo strato rientra nel cosiddetto *SaaS* layer.

C'è da notare come alcuni requisiti essenziali, quali ad esempio:

- la scalabilità delle interconnessioni delle "Cose",
- la loro interoperabilità,
- la gestione dei dati secondo i nuovi criteri dell'App Economy,
- la possibilità di attivare le risorse al "volo" e nella quantità desiderata

rendono necessario l'inserimento di uno strato di disaccoppiamento tra "Cose" ed applicazione che è chiamato con diversi nomi: Platform Tier o Platform as a Service (PaaS) o Device Layer. Di seguito Piattaforma o Piattaforma IoT.

Diversamente dai sistemi tradizionali, la Piattaforma si smaterializza, trovando la sua naturale collocazione nel contesto del "Cloud". Infatti, è nel paradigma del "Cloud Computing" che si ritrovano i requisiti fondamentali di scalabilità, interoperabilità, ubiquità e sicurezza. Anche dal lato applicativo si vede come sia stato necessario disaccoppiare i dati provenienti dalle "Cose" attraverso gli IoT Gateway dalle applicazioni stesse, tramite una piattaforma IoT sul "Cloud".

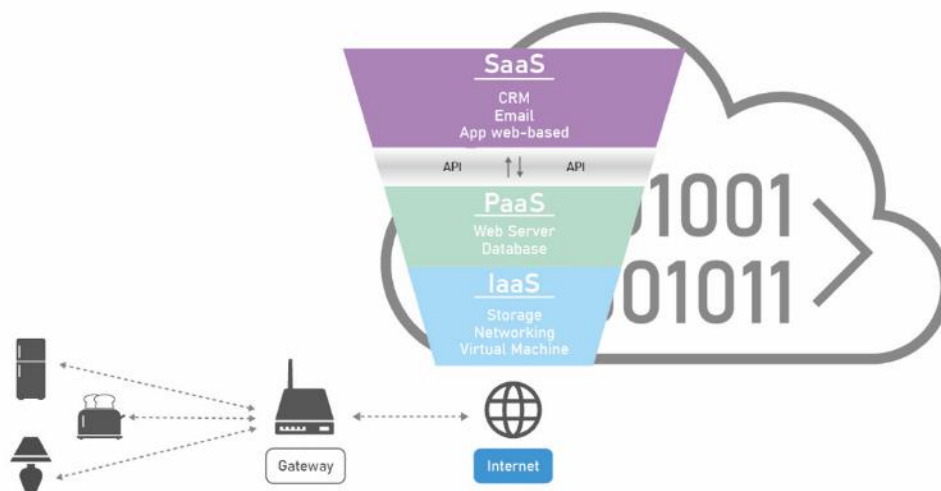


Figura 12: IaaS, PaaS e SaaS

Ripercorrendo a ritroso i passaggi si vede che sul campo si instaura una relazione simbiotica tra “Cose” e Gateway che trova un parallelo a livello “Cloud” tra le App e la Piattaforma. Ne consegue che in una architettura IoT, tra un sensore/attuatore ed una App bisogna inserire un IoT Gateway (implementato in hardware o via software¹³) ed una Piattaforma IoT. Questi due elementi eliminano la complessità nella costruzione di una soluzione IoT rendendo trasparenti tutti gli altri livelli e liberando dati e applicazioni in una flessibilità senza precedenti. I dati, prima imprigionati in Data Silos e applicazioni monolitiche, trovano grazie alla Piattaforma e al suo Data Lake una nuova espansione aprendosi un varco nell’App Economy.

Scalabilità dei sistemi IoT

Scalabilità, Internet, Cloud

Si è detto in precedenza che una delle caratteristiche intrinseche di una architettura IoT è la scalabilità. Tradizionalmente, la realizzazione di un sistema distribuito, come lo è un sistema IoT, richiedeva alcuni passaggi ben definiti: la realizzazione di un prototipo, la successiva creazione di un progetto pilota con poche installazioni di prova, una graduale espansione dello stesso ed infine la distribuzione di massa.

A prima vista, questo processo è ottimale, dal momento che il rischio (errori architetturali, possibili bug hardware e software, problematiche di sicurezza, scalabilità dei software nel data center, problemi con l’interfaccia utente, etc.) verrebbe gestito man mano che il prodotto o servizio viene raffinato e testato in un numero di casi via via più grande. Purtroppo, questo scenario nasconde una difficoltà di fondo: raramente l’infrastruttura di comunicazione sottostante resta immutata durante le fasi dello sviluppo. Ciò comporta numerosi problemi di consistenza e potenzialmente apre la strada a nuovi tipi di bug.

Le architetture IoT, al contrario devono tipicamente essere in grado di servire un numero estremamente grande di utenze e devono processare le transazioni con una frequenza molto elevata.

Questo risultato è stato ottenuto suddividendo una architettura complessa come quella delineata nei precedenti paragrafi in un numero di strati tecnologici indipendenti e interconnessi tra loro con protocolli e metodiche standardizzate, così che il cambio del singolo sottosistema non comprometta la funzionalità del tutto, a condizione che le interfacce tra le parti siano note ed immutabili. Lo strato dei Gateway è caratterizzato dalla massima eterogeneità per quanto riguarda l’interfaccia con il mondo reale e dalla massima omogeneità nelle modalità di aggancio alla rete di telecomunicazione. L’altro strato, la rete di telecomunicazione che si presuppone basata su protocollo Internet (il cosiddetto protocollo TCP/IP), grazie al livello di astrazione del TCP/IP si preoccupa di gestire in modo del tutto trasparente i dettagli che comunica al di sopra di una qualsiasi combinazione di tecnologie – siano esse connessioni in rame o in fibra o wireless - e topologie.

¹³ Naturalmente una implementazione esclusivamente software di un IoT Gateway (o di un IoT Agent) è sempre possibile, in particolare laddove le risorse di calcolo e di memoria del sensore siano adeguate.

Esistono numerosi esempi di come il Cloud sia in grado di offrire una soluzione ottimizzata da un punto di vista economico, quanto robusta da un punto di vista tecnico: servizi come quelli dedicati allo streaming video di eventi dimostrano come sia possibile gestire picchi di traffico estremo su larghissima scala. Il Cloud supera l'antico concetto di hosting o farming, stratificando al di sopra di esso tutta una serie di servizi che consentono di partizionare, distribuire e coordinare tanto il calcolo quanto le transazioni.

Esempi di questi servizi sono i "Load Balancers", che bilanciano e smistano il traffico dei dati in entrata ed uscita senza creare ingorghi ma senza effettuare elaborazione sui dati stessi; i "Brokers", che si occupano della prima analisi dei pacchetti di dati e della loro gestione in code, in funzione dell'ordine di arrivo e del loro instradamento verso i programmi che ne hanno fatto richiesta; i "Database" (relazionali e non), che consentono di conservare in modo ordinato e non volatile i dati al fine di un loro utilizzo successivo, e tanti altri servizi ancora.

Sarebbe tuttavia limitativo pensare che il Cloud sia costituito unicamente dai servizi precedentemente illustrati e dal software che fa da "collante": oltre a questi componenti, che ne costituiscono gli "ingranaggi", nel Cloud troviamo anche protocolli e paradigmi di programmazione, che consentono di realizzare applicazioni e, cosa ancora più importante, di consumare i dati come se fossero dei prodotti semilavorati che possono essere facilmente utilizzati come "materia prima" da un'altra applicazione basata sul Cloud. Tra questi servizi ci sono le API o Application Program Interface, ovvero metodi per riuscire a scambiare dati tra il Cloud e altri programmi residenti nel Cloud stesso o con le WebApp dei nostri Computer e soprattutto con le App dei nostri smartphone.

Le API più note sono le REST (REpresentational State Transfer), ovvero metodi di scambio dati che si basano sugli stessi principi con cui vengono generate le pagine web a partire da un indirizzo IP del sito a cui si vuole accedere. Mettendo assieme tutti questi elementi si comprende come, ad esempio, il dato grezzo proveniente da un ricevitore GPS collocato su un veicolo possa essere "incanalato" nel Cloud attraverso un Gateway, e di qui proseguire il suo viaggio nel Cloud attraverso un Broker e poi un Database. Il dato relativo alla posizione è a questo punto un semilavorato, altamente standardizzato e facilmente consumabile, tramite REST API, da altre applicazioni, come ad esempio un servizio di cartografia che ne restituisca la posizione su una mappa. Il fatto che i dati siano disponibili con chiamate REST permette facilmente il loro uso senza doversi preoccupare di sapere come arrivare a contattare (attraverso il Cloud e le reti di telecomunicazioni il Gateway al quale è attaccato) il ricevitore GPS e senza dover conoscere tutti i vari protocolli di instradamento che servono per raggiungere il GPS stesso; un altro enorme beneficio offerto è che non è assolutamente necessario conoscere le caratteristiche tecniche di accesso al GPS ed alle informazioni in esso contenute, dal momento che con le chiamate REST si accede direttamente al dato.

Come si vede un impianto IoT consente di semplificare drasticamente l'accesso ai dati, consentendo così una scrittura veloce delle applicazioni. Non a caso si parla di App Economy, ovvero dell'insieme di attività economiche che derivano dal grande successo delle applicazioni che utilizzano il Cloud, ed in particolare delle applicazioni mobili. La App Economy non solo comprende la vendita delle applicazioni, ma include anche la pubblicità, la vendita dei dispositivi su cui vengono eseguite le App

ed in generale tutte le fonti di redditività collegate in modo diretto o indiretto al Cloud. Secondo una ricerca di mercato di App Annie del 2018¹⁴, nel 2022 la App Economy registrerà 258 miliardi di download di App all'anno, con una crescita del 45% rispetto al 2017, con un fatturato di 157 miliardi di dollari spesi negli App Store (+92% rispetto al 2017).¹⁵

L'avvento della Industry 4.0

L'Internet of Things come fondazione della Industry 4.0

Il termine "Industry 4.0" ha le sue origini in un progetto¹⁶ del governo tedesco che mirava a promuovere l'informatizzazione del settore manifatturiero.

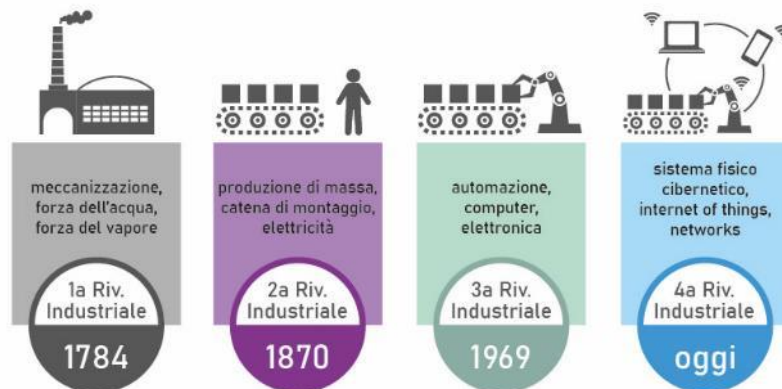


Figura 13: Industry 4.0 e le precedenti rivoluzioni industriali

Volendo tracciare un percorso storico¹⁷, l'avvento della prima industrializzazione coincide con l'introduzione del telaio meccanico (1784) ed è basata sulla produzione meccanica (impianti a vapore e ad acqua) invece che manuale (artigianato).

La seconda industrializzazione nasce con l'introduzione della prima catena di montaggio (1870), segnando così il passaggio ad un partizionamento delle fasi lavorative e all'uso dell'energia elettrica.

La terza industrializzazione risale al 1969, con l'introduzione del primo dispositivo programmabile (PLC). In questa fase i processi vengono automatizzati grazie all'elettronica e all'informatica.

¹⁴ <https://www.appannie.com/en/insights/market-data/app-annie-2017-2022-forecast/>

¹⁵ La Commissione UE ha di recente presentato la proposta di uno specifico regolamento - Com (2017)495, pubblicata il 13 settembre 2017 - finalizzato ad eliminare gli ostacoli alla libera circolazione dei dati non personali. Infatti, come indicato nella comunicazione "Costruire un'economia dei dati europea", una loro maggiore circolazione supporterebbe più efficacemente lo sviluppo delle nuove tecnologie digitali, come il *Cloud computing*, i megadati, l'intelligenza artificiale e l'*Internet of Things (IoT)*, migliorando i servizi offerti agli utenti a tutti i livelli e in tutti i settori.

¹⁶ Germany: Industrie 4.0 – Digital Transformation Monitor – Report (European Commission) - https://ec.europa.eu/growth/tools-databases/dem/monitor/sites/default/files/DTM_Industrie%204.0.pdf

¹⁷ Development of an Assessment Model for Industry 4.0: Industry 4.0-MM - https://www.researchgate.net/publication/319640255_Development_of_an_Assessment_Model_for_Industry_40_Industry_40-MM?_sg=B8W-kJgkTGQZ8E0n_UPgYOcmup12Cj0WCmR5N4uHorr-58MJZn2cIBA_TVz5PctegWU4hD7H_f5rE_FgD52rhUL5QghWAYRkhW

La quarta industrializzazione sta prendendo forma al giorno d'oggi, ed è basata sui quattro principi¹⁸ di una sorta di “manifesto”: l'interoperabilità dei dispositivi, la trasparenza dell'informazione, il supporto alla decisione (“assistenza tecnica”) e la decentralizzazione delle decisioni.

Un altro modo più concreto per descrivere la direzione in cui l'Industry 4.0 si sta muovendo è osservare gli effetti; si parla dunque di “**servitization**” ovvero del passaggio ad una economia in cui la creazione del valore non sia più legata esclusivamente al possesso bene, ma anche ed in larga misura alla sua fruizione. In una situazione tradizionale, il bene viene posseduto esclusivamente ed indipendentemente dal suo effettivo utilizzo; ad es. una automobile viene normalmente acquistata e se ne fruisce solo per una frazione minima di tempo. L'auto è un caso tipico di come un modello di servizio anziché di possesso potrebbe migliorare la vita a tutti riducendo i tempi morti per trovare parcheggio, inquinamento, sprechi di materia ed energia. Per passare però dal possesso al servizio serve che si arrivi all'auto autonoma, così che sia possibile riposizionare la vettura in funzione dell'utilizzatore. Una vettura a guida autonoma rompe il vincolo possesso-fruizione poiché non è necessario che la operi un conducente, e quindi cade anche la principale barriera alla sua fruizione: essendo autonoma può essere sfruttata in qualsiasi istante e potenzialmente da chiunque sia autorizzato ad accedervi. A valle di ciò c'è poi una ulteriore conseguenza: nel momento in cui esistesse un parco di veicoli in grado di operare in piena autonomia, le motivazioni che spingono al possesso del bene si indeboliscono o addirittura scompaiono: in quel preciso momento avviene il passaggio dal possesso del bene alla fruizione del bene-servizio. Questo è solo un esempio eclatante di servitization, ma tutta l'industria dei beni materiali è soggetta a questa transizione dal possesso all'uso.

Perché questo passaggio avvenga, oltre alla robotizzazione delle macchine servono i dati delle macchine. I dati sono gli artefici di questa transizione e di conseguenza non c'è da stupirsi che l'IoT si stia affermando sempre più. L'IoT è l'infrastruttura che genera i dati ed è quella necessaria per realizzare l'Industry 4.0.

Esempi di utilizzo di IoT

I benefici dell'IoT in situazioni concrete

Per sua natura, l'IoT è estremamente versatile e potenzialmente applicabile ad innumerevoli settori; per la numerosità delle possibili installazioni, gli “Smart Building” sono un esempio estremamente rilevante di utilizzo dell'IoT. Si tratta di una vasta gamma di casi d'uso, che includono le abitazioni, gli uffici, le RSA, le aree destinate al commercio, gli impianti industriali e molto altro ancora.

Indipendentemente dalla destinazione d'uso, uno “Smart Building” abilita tramite l'IoT la realizzazione di significativi miglioramenti in aree quali la manutenzione, dove grazie ad un monitoraggio diffuso è possibile ridurre i costi operativi (ottimizzazione dei servizi di riscaldamento, gestione aria condizionata, etc.) e migliorare la qualità del servizio (mediante la manutenzione preventiva). Anche la sicurezza dell'edificio e dei suoi occupanti, così come il loro benessere, possono beneficiare grandemente delle capacità di raccolta dati e di intervento remoto che sono

¹⁸ Design Principles for Industrie 4.0 Scenarios - <https://ieeexplore.ieee.org/document/7427673/authors>

resi possibili dall'IoT. Esiste poi tutta una nuova serie di servizi, ad oggi forse impensabili, che potrebbero nascere dai dati messi a disposizione dall'edificio.

Nella **casa connessa**, ad esempio, i vari dispositivi (allarme, luci, riscaldamento, elettrodomestici) si coordinano e modellano il loro funzionamento in risposta alle abitudini degli abitanti, offrendo al tempo stesso la possibilità di ottimizzare automaticamente la performance dell'edificio nel suo complesso (ad es. favorendo l'illuminazione naturale in luogo di quella artificiale, o disattivando i servizi nelle aree e nei periodi in cui non vi sono degli occupanti). Anche nella casa, la disponibilità di sensori e dati può dar luogo a nuovi servizi di assistenza degli anziani o di soggetti deboli. Con la **telemedicina** poi, la casa potrebbe diventare un'estensione dell'ospedale riducendo così il tempo di ospedalizzazione con benefici sia per quanto riguarda la qualità della vita che i costi.

Ci sono poi esempi di impieghi più verticali dell'IoT che sono specifici di alcune categorie di edificio; per esempio, nel settore industriale l'Internet of Things consente il tracciamento degli asset e delle persone; permette di assicurare il flusso dei beni, coordina diverse fasi di lavorazione, protegge la merce e ne verifica le condizioni di trasporto, fornisce i dati su cui definire metriche per ulteriori analisi.

La cosiddetta **"Connected Industry"** è uno degli ambiti con elevata penetrazione dell'IoT: le "Cose" connesse hanno una natura estremamente variabile, che va da semplicissimi sensori, fino a dispositivi complessi come stampanti, gru o addirittura interi stabilimenti. All'interno della "Connected Industry", il settore dell'Oil & Gas ha una importanza molto rilevante, dovuta soprattutto alla complessità della gestione, controllo ed ottimizzazione degli impianti remoti.

Un altro esempio viene dalle cosiddette **"Smart Cities"**, in cui l'IoT è l'elemento abilitante per una implementazione efficiente di una gamma molto ampia di servizi, che vanno dalla gestione del traffico (**"Smart Traffic"**), alla raccolta di informazioni per la bollettazione (**"Smart Utilities"**), alla sicurezza fisica delle persone (**"Smart Security"**) includendo anche progetti molto verticali, come quelli relativi al monitoraggio ambientale e alla sicurezza del territorio.

Altro esempio da citare è quello della **"Smart Grid"**, che riguarda in particolare la rete elettrica. Si tratta di una applicazione estremamente sensibile che mira al rinnovamento di una infrastruttura complessa che spesso, così come è, preclude l'introduzione di tecnologie innovative, come la produzione distribuita da fonti rinnovabili (ad es. i pannelli solari residenziali).

Anche il futuro dell'industria automobilistica sembra essere indissolubilmente legato all'IoT: le **"Connected Cars"** sono già una realtà concreta, con il monitoraggio, la diagnostica remota, il **"Fleet Management"** e prodotti assicurativi basati sull'uso effettivo del mezzo; a ciò si aggiungono i settori emergenti del V2V ("Vehicle to Vehicle") e del V2X ("Vehicle to Everything"), in cui le comunicazioni tra veicoli e, più in generale, tra i veicoli e tutto ciò che li circonda, promettono di rivoluzionare il mondo dei trasporti; ad esempio, con l'introduzione delle reti 5G e delle comunicazioni V2V sarà possibile creare nuove modalità di guida autonoma ed aumentare significativamente la sicurezza dei passeggeri: si stima che con il passaggio da 4G a 5G, la latenza della comunicazione tra veicoli verrà drasticamente ridotta, e di conseguenza il tempo necessario per reagire ad una richiesta di frenata di emergenza da parte di un veicolo che precede, aumentando significativamente la sicurezza dei passeggeri.

L'elenco degli esempi di utilizzo dell'IoT è troppo lungo per poterne dare una copertura esaustiva, ma vale sicuramente la pena di citare la **"Smart Agriculture"**, la **"Connected Health"**, lo **"Smart Retail"** e la **"Smart Supply Chain"**.

Il concetto di Digital Twin

Dal sistema fisico al suo gemello virtuale

Mentre la terminologia è cambiata nel tempo, il concetto di base del modello Digital Twin è rimasto abbastanza stabile dal suo inizio nel 2002¹⁹. Si basa sull'idea che un costrutto informativo digitale su un sistema fisico potrebbe essere creato come entità autonoma a partire dal sistema fisico stesso. Queste informazioni digitali sarebbero un "gemello" delle informazioni incorporate nel sistema fisico e sarebbero collegate con quel sistema per il suo intero ciclo di vita. Il concetto del gemello digitale risale ad una presentazione dell'Università del Michigan all'industria nel 2002 sul Product Lifecycle Management (PLM).

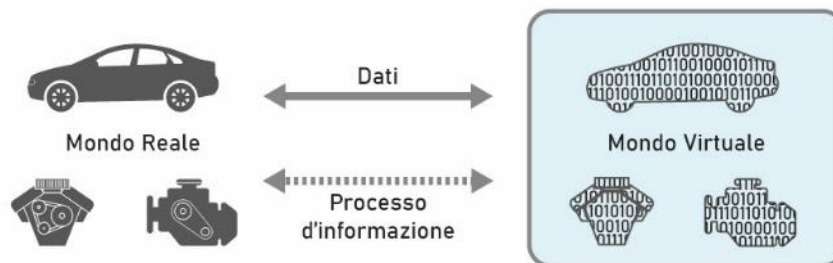


Figura 14: Spazio reale e virtuale

La slide proiettata dal Dr. Grieves, come mostrato in figura, era semplicemente chiamata **"Conceptual Ideal for PLM"**. Tuttavia, aveva tutti gli elementi del Digital Twin: spazio reale, spazio virtuale, collegamento per il flusso di dati dallo spazio reale allo spazio virtuale, il collegamento per il flusso di informazioni dallo spazio virtuale allo spazio reale e ai sottospazi virtuali. La premessa alla base del modello era che ogni sistema consisteva di due sistemi, il sistema fisico che è sempre esistito e un nuovo sistema virtuale che conteneva tutte le informazioni sul sistema fisico. Ciò significava che c'era un mirroring o un gemellaggio di sistemi tra ciò che esisteva nello spazio reale a ciò che esisteva nello spazio virtuale e viceversa. Il PLM o Product Lifecycle Management del titolo significava che questa non era una rappresentazione statica, ma che i due sistemi sarebbero stati collegati durante l'intero ciclo di vita del sistema stesso. I sistemi virtuali e reali sarebbero risultati collegati mentre il sistema attraversava le quattro fasi di creazione, produzione (fabbricazione), funzionamento (supporto / supporto) e smaltimento. Questo modello concettuale è stato utilizzato nei primi corsi di executive PLM presso l'Università del Michigan all'inizio del 2002, dove è stato definito come **"Mirrored Space Model"**. Il concetto è stato ripreso in un articolo del 2005 (Grieves 2005) e nel libro **"PLM, Product Lifecycle Management: Driving the Next Generation of Lean Thinking"**, dove il modello concettuale è stato chiamato **"Information Mirroring Model"** (Grieves 2006). Il paradigma è stato notevolmente ampliato in **"Virtually Perfect: Driving Innovative and Lean Products through Product Lifecycle Management"** (Grieves 2011), dove il concetto era ancora indicato come modello di mirroring delle informazioni. Tuttavia, è qui che il termine Digital Twin è stato associato a questo

¹⁹ https://www.researchgate.net/publication/307509727_Origins_of_the_Digital_Twin_Concept

concetto, in riferimento al modo in cui il coautore ha descritto questo modello. Data la descrittività della frase, il termine *Digital Twin* è stato usato come base concettuale da quel momento in poi, fino ad essere adottato anche nell'area aeronautica e aerospaziale negli ultimi anni. La NASA lo ha utilizzato nelle proprie roadmap tecnologiche (Piascik, Vickers et al. 2010) e nelle proposte per l'esplorazione dello spazio sostenibile (Caruso, Dumbacher et al. 2010). Il concetto è stato proposto per aerei da caccia e veicoli della NASA di prossima generazione (Tuegel, Ingraffea et al. 2011, Glaessgen e Stargel 2012), insieme a una descrizione delle sfide (Tuegel, Ingraffea et al. 2011) e l'implementazione di as-built (Cerrone, Hochhalter et al. 2014).

Dal punto di vista implementativo, il digital twin di un asset interfacciato ad un gateway IoT può essere rappresentato come un insieme di attributi (variabili, metriche o “channels”) che lo caratterizzano. Questi vengono temporaneamente memorizzati nel gateway per elaborazioni locali (“intelligence at the Edge”) e/o pubblicati dal gateway stesso verso una o più piattaforme applicative (on Cloud o On Premises) dove il gemello digitale prende vita. L'insieme di questi attributi è leggibile e scrivibile in modo che si possa completare il trasporto bidirezionale di questi dati dal mondo reale al virtuale e viceversa (o in altre parole dal mondo OT al mondo IT e viceversa). La sfida degli ultimi anni è fare in modo che il disaccoppiamento fisico/virtuale mantenga un dualismo in cui le due entità si confondano una nell'altra fino a divenire indistinguibili, in un'architettura che debba essere sicura, flessibile e scalabile. A questo punto simulare un processo, un intervento di manutenzione o un qualsiasi scenario fisico può trovare la sua completa espressione a livello virtuale prima di essere riportato sul campo. Ed è proprio qui che ci si deve rendere conto di quali implicazioni potrebbe avere l'invio di un comando di attuazione verso il campo in un'architettura non cyber sicura, se fosse alterato prima di essere spedito o durante la comunicazione. In quest'ottica il Digital Twin è una copia virtuale che deve essere spostata e preservata con la stessa cura, attenzione e sicurezza con cui si trasporta un qualsiasi oggetto di valore, ossia un Asset.

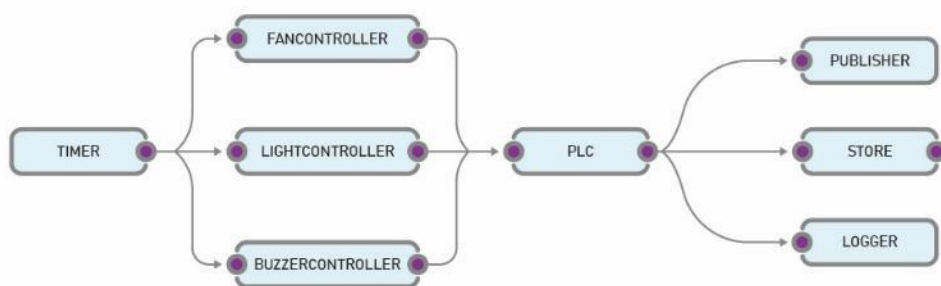


Figura 15: Il concetto di Digital Twin e Asset

Come estrarre valore dai dati prodotti dalle Cose connesse

Dal dato all'analisi, dal Machine Learning all'AI

Così come il fisico ed il virtuale nel digital twin, anche l'IoT e l'analisi dei dati sono due ambiti concettualmente distinti, ma al tempo stesso strettamente correlati, al punto di vivere di una relazione simbiotica.

Infatti, grazie all'IoT è possibile raccogliere enormi quantità di dati con alto contenuto informativo e facilmente manipolabili; tuttavia, in molti casi le dimensioni dei “Data Lake” sono tali da impedire

una analisi umana diretta e per questo motivo è necessario applicarvi degli algoritmi in grado di estrarre il “segnale” dal “rumore”.

Nelle applicazioni più semplici, questo processo può essere gestito con metodi tradizionali: per esempio, identificare un valore sopra una certa soglia non richiede particolari sforzi.

Le applicazioni più interessanti e con valore aggiunto vanno molto oltre questo semplice tipo di analisi: così come l'intelligenza umana riesce a riconoscere schemi nell'apparente disordine, una intelligenza artificiale (**AI - Artificial Intelligence**) può replicare questo processo analitico ed estrarre pattern da un dataset le cui proporzioni siano intrattabili per un essere umano.

Se si prende in considerazione il Quarto Paradigma di Jim Gray²⁰ siamo alle porte di una nuova transizione di fase epistemologica. Il primo e il secondo paradigma sono quelli che Galileo chiamava “sensate esperienze” e “certe dimostrazioni”, ovvero l'osservazione empirica e la teoria, possibilmente matematizzata. L'avvento del computer ha inaugurato una nuova possibilità di produrre nuova conoscenza scientifica, la **simulazione**. Oggi molte ricerche scientifiche riguardano non il mondo naturale, ma un mondo simulato. Lo svantaggio è che i risultati riguardano non la realtà, ma un'approssimazione più o meno buona della realtà. Il vantaggio è che si possono ripetere esperimenti controllati all'infinito, modificando i parametri e navigando a piacimento nello spazio e nel tempo. Ebbene, sostiene Jim Gray, il quarto paradigma consiste nel navigare in un mare sconfinato di dati alla ricerca (anche) di ordine e regolarità che non vediamo e che le teorie non prevedono. Si tratta di una navigazione interdisciplinare capace di generare nuova conoscenza.

Negli ultimi anni le tecniche di AI stanno avendo un grande impulso anche grazie all'avvento dell'IoT, in virtù della possibilità di disporre di dataset ampi e ricchi di contenuti: questa positiva e reciproca contaminazione sta dando grandi risultati e ha attivato un ciclo virtuoso di mutua accelerazione.

L'Artificial Intelligence si dirama in varie discipline e tra queste il Machine Learning (ML) sta riscuotendo molto interesse, in particolare nella sua accezione del Deep Learning, in cui il sistema è in grado di apprendere autonomamente e grazie alle reti neurali viene creato un modello che può generare inferenze direttamente sul campo.

Un esempio di come la combinazione di Intelligenza Artificiale (in una delle sue forme) consenta di trattare in modo fine problemi estremamente complessi è la manutenzione preventiva nel settore aeronautico. In questa applicazione, lo scopo è la massimizzazione della disponibilità del velivolo e della sua puntualità: si tratta di un problema difficile da trattare a causa del gran numero di parametri (alcuni indipendenti, altri correlati) che concorrono a definire lo stato del velivolo.

Ma questo è solo l'inizio di una serie di applicazioni che partono da alcuni mercati di nicchia dove la digitalizzazione è già avvenuta. Con gli elettrodomestici smart e gli impianti tecnologici smart, le applicazioni dell'Intelligenza Artificiale si estenderanno fino al settore residenziale e del building in generale. Volendo spingerci ancora oltre si potrà arrivare ad un tale livello di intelligenza in cui, come in parte ipotizzato da Jim Gray, saranno le reti stesse a crearsi schemi e dataset simulati in modo che classi e contesti non noti a priori possano essere appresi automaticamente (unsupervised learning)²¹.

²⁰ <https://www.scienzainrete.it/contenuto/articolo/quarto-paradigma>

²¹ https://en.wikipedia.org/wiki/Unsupervised_learning

Data economy e il significato dei dati

*Come evidenziato nel capitolo precedente, diversi studi di mercato di App Annie²² confermano la crescita esplosiva dell'economia globale delle App nei prossimi anni. La base di utilizzatori di App²³ quasi raddoppierà dal 2017 al 2022, passando da 3,9 miliardi a 6,1 miliardi. Anche il tempo trascorso nell'uso delle App continuerà a crescere passando dai 1600 miliardi di ore del 2011 ai 3500 miliardi di ore del 2021. Le architetture IoT, per potere stare al passo con i tempi, dovranno quindi basarsi sugli stessi paradigmi architettonici dei dispositivi mobili. Ecco perché l'architettura IoT presentata in questo libro è stata basata su una piattaforma IoT che è installata sul Cloud e che si interfaccia da una parte con i Gateway sul campo e dall'altra con le Applicazioni tramite chiamate REST. I programmi, ovvero le App scambiano dati con le Cose tramite REST API, quindi con lo stesso schema con cui si scrive la stragrande maggioranza delle applicazioni per i dispositivi mobili. Questo significa che i costi per scrivere le applicazioni IoT risultano essere contenuti e si viene a sviluppare inoltre un App store contenente applicazioni dedicate ciascuna ad uno specifico problema. Inoltre, se le API vengono rese disponibili, gratuitamente o a pagamento, si possono abilitare ecosistemi di sviluppatori, ovvero soggetti terzi senza competenze specifiche, ad esempio, di building automation, che a loro volta possono scrivere nuove App incrociando i dati IoT con dati provenienti da altre piattaforme. Rendere disponibili le API sulle le piattaforme IoT consente anche a produttori di dispositivi con bus di campo proprietario di poter scambiare i dati provenienti dal campo a livello di Cloud risolvendo i molti problemi di incomunicabilità presenti tra dispositivi prodotti da costruttori diversi che rendono difficile il compito del System Integrator. L'apertura delle API potrebbe pertanto rappresentare una grossa opportunità per una concreta evoluzione verso l'Edificio digitale e per una maggiore diffusione della building automation, che non c'è dubbio sia stata almeno in parte rallentata dai problemi di interoperabilità. Con l'App Economy si possono attivare nuovi modelli di produzione e consumo dei dati anche in ambito Edificio, come: **servitization, prosumerization e gamification**.*

Le principali categorie di dati IoT

Il dato e la sua monetizzazione

La quantità dei dati generati non solo è immensa ma aumenta in modo esponenziale. Inizialmente questi dati venivano alimentati dalle nostre linee fisse, telefoni cellulari, computer e dispositivi simili. Attualmente invece i dati arrivano da numerosi fonti e sono appunto le "Cose" connesse alla Rete che li generano.

Il passaggio da un prodotto fisico complesso a un sistema connesso che combina i sensori, i software e l'interfaccia dell'utente sta creando uno spostamento del valore che le aziende non possono ignorare. Il vero valore non sta più solo nel prodotto, ma anche nelle opportunità che possono emergere in termini di nuove informazioni ottenibili dai dati generati dai dispositivi e dai nuovi

²² <https://www.appannie.com/en/insights/market-data/app-economy-forecast-6-trillion-market-making/>

²³ <https://www.appannie.com/en/insights/market-data/app-annie-2017-2022-forecast/>

modelli di business, senza escludere il miglioramento dell'esperienza d'uso o fruizione dei prodotti stessi.

Nonostante la quantità dei dati raccolti e da raccogliere sia immensa, quelli che oggi vengono monetizzati possono essere classificati in un numero limitato di gruppi.



Figura 16: Le principali categorie di dati da monetizzare

Localizzazione

Si basa sulla possibilità di individuare il punto esatto dove si trova qualcuno o qualcosa. Tipicamente la localizzazione avviene tramite GPS, Wi-Fi, Cell-ID, o semplicemente chiedendo all'utente la sua posizione.

Ambiente

Si basa sulla misura e la raccolta delle variabili meteorologiche e ambientali. Un esempio in questo senso è rappresentato dal settore agricolo. Un'azienda agricola decide di munirsi di sensori per capire lo stato della raccolta e prevedere le condizioni meteo. I dati così raccolti vengono utilizzati dall'azienda stessa per ottimizzare il proprio core business (semina, raccolta, irrigazione, disinfestazione). Le stesse informazioni possono essere veicolate ad un sistema di partner che le utilizzano a loro volta per la gestione del loro core business:

1. Dati ambientali, ad aziende specializzate in previsioni meteo;
2. Dati sulla qualità e quantità della produzione, ad aziende chimiche specializzate nella produzione di pesticidi.

Macchine

Si basa su dati che vengono generati in automatico dai macchinari senza chiedere l'intervento umano. Ad esempio, i sensori posizionati all'interno di un'auto possono percepire la velocità di guida, l'accelerazione, la rottura dei freni, l'usura delle ruote e una serie di altre informazioni. Questi dati vengono utilizzati in primis dal produttore della macchina per ottimizzare i propri cicli di manutenzione, anche preventiva, e individuare le eventuali aree di miglioramento per lo sviluppo futuro della macchina. Allo stesso tempo gli stessi dati possono essere messi a disposizione di un ecosistema di partner, tra cui:

1. Il produttore dei singoli componenti, per migliorare le prestazioni;
2. Aziende di servizi, ad esempio le assicurazioni per la proposizione di prodotti "tailor-made" sul reale utilizzo delle macchine.

Salute

Si basa su dati raccolti dai sensori che monitorano il nostro corpo (sangue, pressione, temperatura, battito cardiaco, ecc.). Le aziende farmaceutiche, partendo da dati resi anonimi, possono fare ricerche per realizzare prodotti migliori.

Movimento

Si basa sul movimento o la posizione di un essere umano o di un oggetto rispetto ad un modello ideale. Ad esempio, la possibilità di utilizzare dispositivi e sensori come trainer, durante il periodo di convalescenza di una persona che ha subito un incidente.

Gli attori costituenti l'ecosistema

I principali attori dell'ecosistema dei dati sono²⁴:

1. I generatori dei dati;
2. I fornitori dei data services;
3. Data business user;
4. Gli utenti finali.

I generatori dei dati

Questi sono la primaria fonte dei dati: il browser Internet degli utilizzatori, i consumatori che pagano con la loro carta di credito, la localizzazione da una lettura del GPS, un sistema intelligente con la funzione di ridurre il consumo dell'energia all'interno delle nostre case, o semplicemente la pioggia in una giornata estiva. Ogni azione volontaria e non, generata da esseri umani e non, convertita in informazione digitale che può essere raccolta e aggregata per analisi di dati.

I fornitori di data services

La vera creazione del valore avviene solo quando l'informazione è processata e analizzata. Questo include la sua raccolta, l'organizzazione, l'immagazzinamento, la consultazione, l'uso, la trasmissione, la distruzione ecc.

Nella figura sotto viene schematizzata la catena del valore della creazione di un data service.

²⁴ European Political Strategy Centre (EPSC): Enter the Data Economy

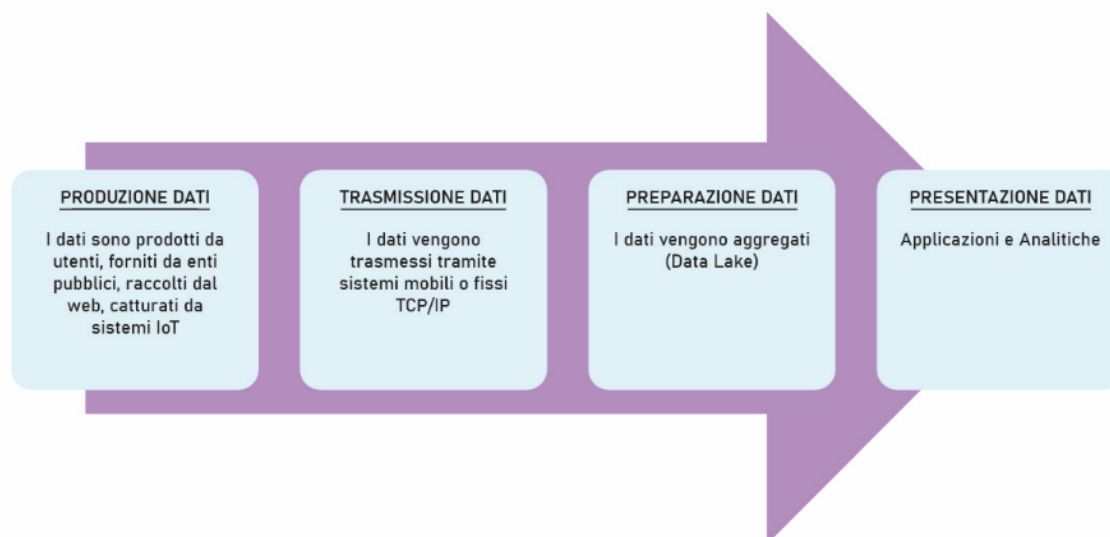


Figura 17: Catena di valore nella generazione dei dati

Data business user

Queste sono le aziende e la pubblica amministrazione che utilizzano i risultati del data analytics per migliorare le performance.

I consumatori finali

L'ultimo gruppo di attori sono gli acquirenti a valle; i consumatori, i consumatori business, i cittadini che hanno a che fare con quelle aziende o quella pubblica amministrazione che hanno implementato l'analisi big data al loro interno.

Nella tabella sotto si trovano alcuni dei benefici, rischi e colli di bottiglia che si ottengono dai dati per ogni tipologia di attore.

ATTORI	BENEFICI	RISCHI/COLLI DI BOTTIGLIA
GENERATORI DI DATI	- Capacità di utilizzare i propri dati come commodity	- Violazione della sicurezza - Violazione della privacy
DATA SERVICES	- Generazione del profitto	- Collo di bottiglia nel flusso dei dati - Costi di conformità del quadro normativo
UTILIZZATORI DEI DATA BUSINESS	- Incremento della produttività - Innovazione incrementale e distruttiva	- Costi di investimento vs incertezza della normativa - Resistenza o incapacità ad implementare analisi big data
CONSUMATORI FINALI	- Bassi prezzi e alta qualità - Offerte su misura - Nuovi servizi/prodotti	- Discriminazione del prezzo - Sicurezza e violazione della privacy

Tabella 1: Benefici e rischi/colli di bottiglia per tipologia di attore

Il valore dei dati nel tempo

Il flusso dei dati ha creato nuove infrastrutture, nuovi business, nuove politiche e una nuova economia. Ha cambiato le regole del mercato e richiede nuovi approcci da parte delle Autorità.

Dall'altro lato anche la percezione della qualità del dato è cambiata. Non ci sono più solo stock di dati digitali, database di dati personali come nome, età e sesso. La nuova economia si occupa di analisi dei flussi di dati in tempo reale, spesso di dati non strutturati. I flussi di video e foto postate dagli utenti dei social network, le informazioni prodotte dai dispositivi nelle ore di attività, le informazioni generate dai sensori delle macchine ecc. Sembra che tutti gli oggetti siano destinati ad essere associati ad un sensore tale per cui le persone anche se non connesse lasceranno una traccia digitale.

La cosa più importante è che il valore dei dati sta aumentando. All'inizio Facebook e Google usavano i dati per semplici operazioni di pubblicità mirate. Negli ultimi anni però hanno compreso che questi dati possono essere trasformati in intelligenza artificiale o servizi "cognitivi", alcuni dei quali generano altre fonti di ricavi. Questi servizi includono la traduzione, il riconoscimento facciale e valutano la personalità in base a quello che le persone scrivono sui social o motori di ricerca; tutte queste informazioni possono essere vendute ad aziende di prodotti.²⁵

Uber è conosciuto come servizio taxi a basso prezzo. Ma se l'azienda vale 80 miliardi di dollari dopo la quotazione in Borsa del 2019 è principalmente dovuto al fatto che possiede il più grande pool di dati sull'offerta (conducenti) e sulla domanda (passeggeri) per il trasporto personale.

Netflix, la popolare piattaforma di streaming americana, ha sfruttato il suo ricco database che registrava le ricerche, le scelte, le pause e le recensioni dei suoi iscritti, per creare la serie digitale House of Cards. La serie ha fatto salire alle stelle la popolarità di Netflix.²⁶

Alex "Sandy" Pentland e il suo gruppo del MIT Media Lab hanno utilizzato i dati di localizzazione dei telefoni cellulari delle persone per dedurre quanta gente si trovasse all'interno dei Macy Store nel giorno del Black Friday, negli Stati Uniti. Così facendo, sono stati in grado di stimare le vendite della catena della grande distribuzione ancor prima della compagna stessa²⁷.

È in particolare in quest'ultimo esempio che si percepisce, tra le altre, anche l'importanza dell'analisi dei dati real-time.

Modelli di business²⁸

Oggi il modello di business di un'azienda dipende fortemente dalle tecnologie che vengono usate. Ci sono infatti imprenditori che hanno creato nuovi business model che derivano interamente dalle tecnologie esistenti o emergenti. Usando le tecnologie le aziende possono raggiungere un ampio numero di clienti a costi ridotti. Nonostante ci sia un'ampia varietà di business model possibili, questi possono essere raggruppati in tre principali categorie: modello di business lineare, il modello Platform-based e il modello ibrido.

In un modello di business lineare le operazioni all'interno dell'azienda sono ben descritte dalla tipica catena di fornitura lineare. Le aziende con un business model lineare creano valore sotto forma di beni o servizi e poi li vendono a qualcuno a valle nella loro catena di fornitura. Il modello di business

²⁵ The Economist: Data is giving rise to a new economy

²⁶ Il Sole 24 Ore: Raccolta, elaborazione e utilizzo delle informazioni in rete sono il petrolio del futuro

²⁷ Harvard Business Review: Big Data The Management Revolution

²⁸ <https://www.applicoinc.com/blog/what-is-a-platform-business-model/>

lineare si differenzia poi tra B2B (Business2Business), B2C (Business2Consumer) e E2E (Everything2Everyone).

In un modello Platform-based si crea valore facilitando gli scambi tra due o più gruppi indipendenti, in genere consumatori e produttori. Tra l'altro, è importante precisare che non tutte le aziende tecnologiche propongono un modello di business basato su una Platform. Netflix, ad esempio, non ha un modello Platform-based; essa infatti ha un modello di business lineare e le sue operazioni sono ben descritte dalla tipica catena di fornitura E2E.

Alcune aziende come Apple e Amazon adottano un approccio ibrido che combina modelli di business lineari e Platform-based. Sebbene un modello ibrido non sia adatto a tutte le aziende, quando ciò è possibile può essere molto efficace e redditizio.

Amazon ad esempio ha un modello ibrido nel suo business dell'e-commerce B2C. L'azienda inizia a vendere libri basandosi su un modello di business lineare. Il merito della gran parte della sua popolarità però, è data dalla combinazione del suo approccio lineare con Amazon Marketplace, che consente ai venditori di terze parti di vendere articoli.

All'interno di queste tre categorie si può poi ulteriormente suddividere il modello in base alla vendita di prodotti o di servizi. Con il digitale si sta assistendo ad un grande cambiamento di che cosa viene venduto, ovvero si assiste ad un passaggio dalla vendita del prodotto alla vendita del risultato o dell'uso del prodotto.

Dalla Sharing Economy²⁹ all'Outcome Economy³⁰

Se si parla di Platform business model non si può non parlare di Sharing Economy. Il termine Sharing Economy (Economia della condivisione), infatti, descrive un modello basato sulla condivisione di un prodotto o servizio tra più individui. Questo modello è il paradigma del passaggio dal possesso all'uso dei beni ed ha registrato una forte crescita in vari settori a partire dalla crisi economica e finanziaria del 2008, generando opportunità e sfide per imprese e legislatori.

L'evoluzione dell'economia della condivisione è avvenuta attraverso la spinta propulsiva di tre differenti driver: sociali, economici e tecnologici.

I social drivers sono rappresentati dall'aumento demografico che favorisce l'incontro di domanda e offerta di condivisione, dal crescente desiderio di comunicazione e dalla maggiore attenzione verso la sostenibilità ambientale che porta a preferire le logiche "usa e condividi" ed "usa e collabora" rispetto a quella "usa e getta".

I drivers economici hanno come obiettivo l'ottimizzazione di risorse in eccesso o inutilizzate. Sempre tra i driver economici vi sono il desiderio degli individui di maggiore flessibilità nel proprio portafoglio di assets, che porta a preferire per determinati beni una condivisione P2P (peer-to-peer) o meglio un P2P renting dei beni troppo onerosi per essere acquistati a tempo pieno. I drivers tecnologici sono rappresentati infine dalle reti pervasive di telecomunicazioni, dalla disponibilità a

²⁹ http://tesi.cab.unipd.it/53193/1/Landini_Alessandro.pdf

³⁰ The Outcome Economy - How the Industrial Internet of Things is Transforming Every Business - Joseph Barkai

basso costo di calcolatori dotati di interfacce per l'interazione, quali gli smartphone, e grazie al Cloud, la App economy, ed i nuovi sistemi di pagamento elettronico.

La combinazione di questi effetti ha reso possibile il decollo della Sharing Economy, l'economia che aprirà le porte alla servitizzazione delle cose o meglio all'economia del risultato, la così detta **"Outcome Economy"**. Ovvero un'economia in cui la monetizzazione avviene dal risultato prodotto dal bene e non dal bene stesso. Per fare questo passaggio è abbastanza evidente che è necessario conoscere istantaneamente e a distanza lo stato del prodotto. Passare dunque dall'economia della vendita del bene all'economia della vendita del risultato, richiede come prerequisito la digitalizzazione del bene e la sua connessione in modalità IoT alla rete internet.

La Sharing Economy è anche il risultato delle nuove tecnologie del software (dal Cloud all'App Economy) e della pervasività delle reti informatiche e dei calcolatori (Internet e Smartphone) e la quarta rivoluzione industriale ha alla base queste stesse tecnologie. Se poi pensiamo all'auto come paradigma della trasformazione in corso, si può intuire come dall'attuale modello di sharing proposto da società come Uber e con l'avvento della guida autonoma, le stesse case automobilistiche potranno adottare un modello di servizio in cui l'auto non verrà più venduta ma data in uso con un contratto pluriennale di servizio. Non si possiederà più l'auto ma si avrà sempre un'auto a disposizione. La quarta rivoluzione è basata su IoT, Big Data, AI e Cobot (robot collaborativi) e su queste stesse tecnologie si baseranno gli edifici e le città del futuro dove si andranno a mutuare ed amplificare i nuovi modelli di business derivanti dalle stesse tecnologie digitali adottate e che già stanno vedendo la luce in molti ambiti. I modelli economici alla base di questi scambi non sono il vecchio concetto di affitto, e questo non perché facciano uso di piattaforme digitali, ma poiché alla base hanno un innovativo approccio di condivisione. Perché la proprietà dei beni tenderà a rimanere in capo a chi produce i beni? Perché sarà più sostenibile ed economicamente conveniente fare così. Il digitale porta le aziende a pensare in modo circolare e di conseguenza la maggior parte dei beni dovrà essere monetizzata con il risultato che produce.

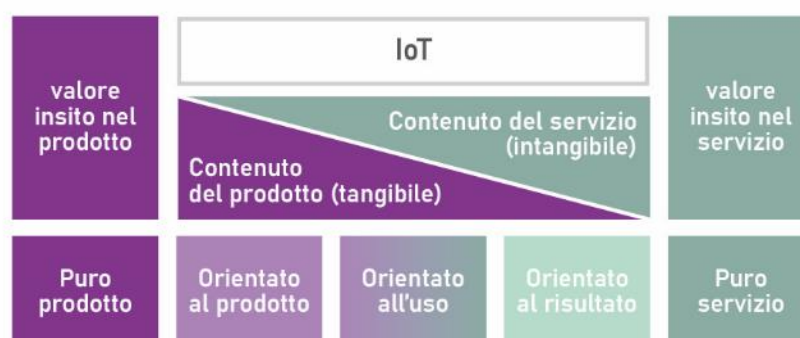


Figura 18: La transizione del Valore da Prodotto a Servizio abilitata dall'IoT

Le norme della Sharing Economy

La Sharing Economy si basa sui dati e senza questi non può svilupparsi; inoltre gli utenti che, proprio con la consapevolezza di voler condividere, mettono a disposizione occasionalmente beni e servizi, sembrano di fatto mettere in atto nuove forme di economia che non sempre si possono inquadrare con le stesse leggi che regolano gli operatori economici del medesimo settore. Questo nuovo modello economico, che è presente in tutto il mondo e sta modificando molto rapidamente le regole del mercato, richiede un adeguamento delle norme fiscali, contrattuali e di riservatezza dei dati.

Dal punto di vista normativo, infatti, nel nostro ordinamento non ci sono norme specifiche. Nell'ottica di una regolamentazione ad hoc, l'Intergruppo Parlamentare per l'innovazione ha preparato una proposta di legge³¹, presentata a marzo del 2016, che Disciplina le piattaforme digitali per la condivisione di beni e servizi e disposizioni per la promozione dell'economia della condivisione.

Il testo della proposta di legge prevede anche un articolo dedicato alla "Tutela della riservatezza" (art.7), il quale sembrerebbe in linea con le disposizioni ex D.Lgs. n. 196/2003 e con le prescrizioni dettate dal Garante Privacy, fornendo una prima definizione di "dato utente". Esso può essere definito come "il dato personale di cui sia stato acquisito il consenso ai sensi del D.Lgs. n.196/2003 e il dato prodotto e ottenuto dall'integrazione digitale di oggetti". Molto importante è l'espresso riferimento all'Internet of Things.

L'art. 7 intende disciplinare anche la cessione dei dati dell'utente a terzi stabilendo che, nei casi in cui il gestore voglia cedere a terzi dati utente del cui trattamento è titolare, deve comunicare ai soggetti cui tali dati utente si riferiscono, entro un tempo congruo antecedente alla cessione, le modalità e i tempi della cessione e consentire ai titolari, contestualmente alla comunicazione, di effettuare, con un solo comando o rispondendo a una comunicazione elettronica, l'eliminazione dei dati che lo riguardano. Il Garante per la protezione dei dati personali avrà il compito di stabilire con propria delibera i requisiti minimi dell'informativa all'utente, il termine per la comunicazione di cessione e il funzionamento del meccanismo di eliminazione dei dati.

Inoltre, le piattaforme digitali dovrebbero sempre garantire a ogni utente uno strumento online di verifica, modifica, obliterazione, cancellazione e prelievo dei propri dati utente con granularità singolare ovvero raggruppati per categorie omogenee o in forma complessiva e la possibilità di cancellare definitivamente, con una sola operazione, tutti i dati memorizzati all'interno del profilo dell'utente. Purtroppo, a quattro anni dalla presentazione della proposta, se ne sono perse le tracce in Parlamento.

Esempi di uso dei dati: il caso dei dati prodotti dalle automobili³²

Le auto genereranno dati su come vengono utilizzate, la loro posizione e chi si trova alla guida. La quantità di informazioni, come si può immaginare, anche in questo mercato sta aumentando in modo esponenziale. La maggior parte di questi dati è generata con un **modello prosumer** (Producer/Consumer), ovvero un modello in cui il consumatore dei dati è a sua volta produttore di dati. Ecco perché molte applicazioni sono solo apparentemente gratuite. Il pagamento di queste

³¹ <http://www.techeconomy.it/2016/03/02/pronta-la-proposta-legge-sulla-sharing-economy/>

³² McKinsey: Monetizing car data New service business opportunities to create new customer benefits

App viene fatto dall'utilizzatore tramite la produzione dei dati che vengono ceduti al produttore della App stessa per l'erogazione del servizio. Il modello prosumer funziona perché i dati che cediamo, per esempio quando usiamo Google Maps o Waze, e che sono la posizione e la velocità della nostra auto, ci danno più vantaggi rispetto al costo percepito di cedere alcuni nostri dati. Ritornando ai dati nel mondo automobilistico, sono 4 i principali macro-trend che stanno alla base della loro produzione: **mobilità elettrica, mobilità condivisa, connettività, guida autonoma**.

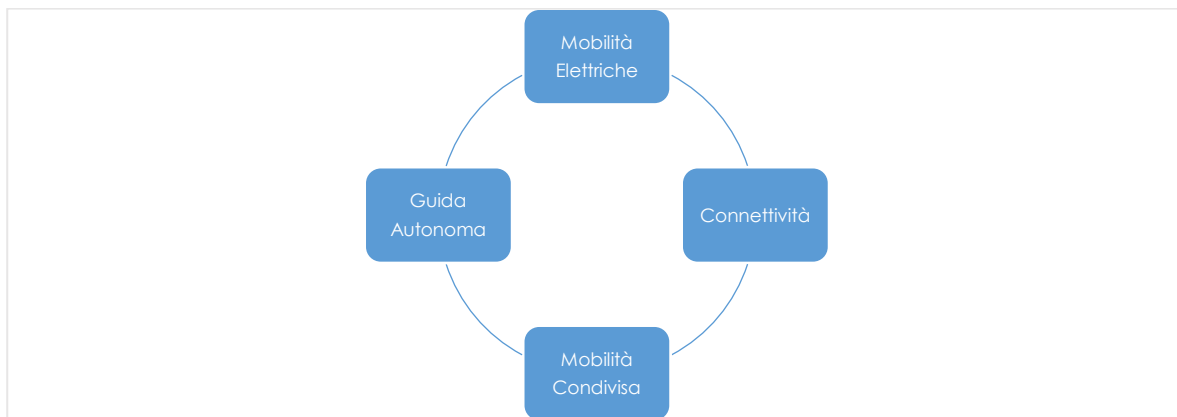


Figura 19: Tecnologie disruptive per il mercato tradizionale delle auto

Mobilità elettrica - Dovuta alla riduzione dei costi delle batterie, disponibilità delle stazioni di ricarica e un incremento di accettazione da parte dei clienti. **Car Sharing** - Un modello di mobilità sempre in crescita. **Connettività** - Nuove funzionalità e caratteristiche vengono offerte ai passeggeri. **Guida autonoma** - L'auto si trasforma in una piattaforma per le attività personali.

Quello che i trend hanno in comune è il loro contributo presente e futuro a un incremento dei dati digitali generati dalle auto non solo per l'industria automobilistica ma altresì per nuovi player. Settori come le assicurazioni, le telecomunicazioni, high-tech ecc. giocheranno un ruolo chiave nell'abilitare servizi a pagamento legati ai dati.

Le figure coinvolte al momento sono: i guidatori conducenti, i venditori di auto, i fornitori automobilistici e le assicurazioni.

I **conducenti** accettano di condividere le proprie informazioni perché sono interessati:

1. Alla loro salute e alla sicurezza: in caso di incidenti le chiamate di emergenza partono in automatico; vengono fornite informazioni su rischi/pericoli permettendo al guidatore di rispondere velocemente;
2. Alla convenienza: permettere al cliente di fare manutenzione preventiva e possibili risparmi sull'assicurazione;
3. Al risparmio del tempo: ottimizzazione dei percorsi e informazione sui parcheggi.

I **venditori delle auto** sono interessati a capire come i clienti usano le auto, le scelte di manutenzione e riparazione, solo per citarne alcune. I **fornitori automobilistici** sono interessati a capire come sfruttare i dati per raggiungere direttamente i clienti finali, come servire meglio i clienti B2B e migliorare il proprio portafoglio prodotti e servizi. Le **assicurazioni** sono interessate a ricostruire la dinamica esatta del sinistro, e fare polizze su misura.

Le macro categorie di dati che vengono generati possono essere classificate come nella Tabella 2 con differenti livelli di sensibilità sulla privacy percepita dal consumatore.

MACRO CATEGORIE	OGGI	2020-25	
Condizioni stradali e ambientali (es. pericolo di scivolamento causa ghiaccio)	- Mappe in tempo reale	- Adozione di sicurezza preventiva - Report sulle condizioni della strada in tempo reale	<div>Sensibilità dati bassa</div> <div>Sensibilità dati alta</div>
Status tecnico del veicolo (es. temperatura dell'olio, stato airbag, report sui malfunzionamenti tecnici)	- Diagnosi di riparazione delle auto - Chiamate di emergenza in automatico	- Predittivo, servizio di prenotazione da remoto	
Utilizzo del veicolo (velocità, localizzazione, peso medio del carico del mezzo)	- Assicurazione su misura - Pagamento in base al percorso	- Riduzione dei costi di ingegnerizzazione	
Diretta comunicazione dal veicolo (calendario, telefono, SMS, e-mail)	- Controllo vocale dei messaggi e delle e-mail.	- Navigazione e servizi proattivi - Assistenza virtuale	

Tabella 2: Livello di sensibilità della privacy percepita dal cliente per categorie di dati

Il valore della Data Economy e le Norme³³

Il valore della data economy in Europa è stato stimato in €285 miliardi nel 2015, rappresentando l'1.94% del PIL Europeo. Con le condizioni politiche e legislative favorevoli e l'incoraggiamento degli investimenti nell'ICT, si stimava questo valore in crescita fino a €739 miliardi nel 2020, rappresentando il 4% del PIL Europeo. L'Unione Europea necessita di assicurare che i flussi dei dati tra i confini e i settori siano disciplinati così che i dati siano disponibili e riutilizzabili per la maggior parte degli stakeholder in modo ottimale. Per far questo le *sfide* che l'Europa dovrà affrontare sono molte e le più importanti sono qui di seguito elencate.

Rimuovere le restrizioni sulla localizzazione dei dati: flusso libero dei dati

Flusso libero dei dati significa avere la possibilità di processare e di immagazzinare i dati in un formato elettronico standard e ovunque all'interno dell'UE. La regolamentazione sul libero flusso dei dati non personali aiuterà a rafforzare la competitività delle imprese europee e a rinnovare ulteriormente i servizi pubblici. L'UE sta cercando di garantire per i dati non personali gli stessi gradi di libertà che il General Data Protection Regulation (GDPR) ha garantito ai dati personali.

Promuovere l'utilizzo dei dati pubblici

L'UE ha pubblicato a giugno del 2019 la direttiva 2019/1024 relativa all'accessibilità e al riuso dei dati pubblici o che derivano da finanziamenti pubblici, che dovrà essere recepita in tutti gli Stati membri entro il 21 luglio 2021. Un primo ma importante passo per rafforzare la data economy Europea, dando alla luce nuovi modelli di business e nuovi lavori.

³³ European Commission: Building a European data economy

Le principali problematiche legate alla data economy

La Commissione Europea ha definito le seguenti questioni e ha avviato un dialogo con le parti interessate:

1. I dati generati dalle macchine non personali devono essere negoziabili per permettere ai modelli di business innovativi di progredire, ai nuovi operatori di mercato di proporre nuove idee e alle start-up di avere una giusta opportunità di competere.
2. Le tecnologie basate sui dati stanno trasformando la nostra economia e la società, con conseguente produzione di quantità sempre maggiori di dati. Questo fenomeno porta a nuovi modi di raccogliere, acquisire, elaborare e utilizzare dati che rappresentano una sfida all'attuale quadro normativo/giuridico.

Elementi di Architetture IoT nell'Edificio

Fino ad oggi i sistemi di automazione di edificio sono stati concepiti come confinati all'interno dell'edificio stesso, seppur in presenza di connessioni remote relegate esclusivamente a fini di supervisione; per tale ragione le interazioni tra dispositivi attraverso differenti protocolli di comunicazione sono state considerate come interazioni a livello di campo. Questo ha prodotto dagli anni '90 ad oggi una competizione per l'affermazione di un protocollo di campo piuttosto che un altro e una aperta discussione su prospettive di convergenza tecnologica verso un unico standard per l'automazione di edificio. Come vedremo nei prossimi paragrafi, tutto questo è cambiato dal momento in cui si è cominciato a parlare di IoT (Internet of Things) e la tecnologia ha dimostrato l'efficacia e la relativa semplicità di poter integrare sistemi eterogenei che possono comunicare tra di loro attraverso nuove architetture software che dal Cloud si sono estese all'IoT.

Pertanto, quello che verrà illustrato nei prossimi paragrafi è un percorso evolutivo del concetto di integrazione tra sistemi di automazione e del concetto stesso di sistema di automazione, percorso che si è sviluppato in 30 anni attraversando numerose e sostanziali innovazioni tecnologiche.

All'interno dell'edificio, i diversi sottosistemi richiedono una gestione integrata che va sotto il nome di BMS (Building Management System) nel quale da una o più interfacce si possano supervisionare e comandare tutte le funzioni dei sistemi BEMS e BACS, funzioni regolabili e modificabili anche a livello locale sotto ogni area dell'edificio mediante ulteriori interfacce locali, gateway e bridge.

Grazie alla diffusione dei sistemi "mobile" e l'aggiunta su quelli di ultima generazione di vari sistemi di identificazione sicura, questi sono ormai eletti ad ospitare l'interfaccia BMS. Infatti, gli Smartphone, grazie all'App Economy, offrono una facile connessione al Cloud ed ospitano già alcune delle tecnologie radio necessarie alla gestione remota dei BEMS e BACS.

Gli strati dell'architettura

L'architettura IoT, come si è visto nel Capitolo: "Cosa significa e le opportunità dell'IoT", è realizzata a strati debolmente accoppiati, a partire dal gateway per arrivare al Cloud e poi alle App dei nostri smartphone. Con "debolmente accoppiato" si intende uno strato che ha con un altro strato pochi e standardizzati metodi di interazione. Lo strato che rimane fortemente "legato", a causa di una moltitudine di standard di comunicazione e di sensori e attuatori diversi è il primo strato, ovvero quello che interconnette il mondo reale con il mondo digitale. In questo strato si collocano i canali di comunicazione e i protocolli di campo che i vari costruttori hanno sviluppato e cercato di standardizzare negli ultimi trent'anni. In questo strato si collocano infine anche tutti i protocolli e le reti a corto raggio dette anche PAN (Peripheral Area Network), tra cui i più noti sono: ZigBee, Z-Wave, Bluetooth nelle varie versioni fino al BLE (Bluetooth Low Energy). Poiché gli edifici sono centrali in questa trattazione, approfondiremo i protocolli di campo in uso nella domotica e nella building automation.

Generalità sui protocolli di campo negli Edifici

La Home & Building Automation, o Domotica in ambito residenziale, è l'insieme degli aspetti di ricerca ed applicativi che si occupano dell'integrazione (ottenuta mediante l'utilizzo dell'elettronica e dell'informatica), dei prodotti, degli impianti e dei servizi che permettono l'automazione delle funzioni negli edifici. Domotica e Building Automation pertanto significa integrare tra loro dispositivi e sistemi diversi, che si scambiano informazioni, ed offrire all'utente una diversa e più razionale modalità di interazione e controllo. Un sistema BACS utilizza una comunicazione digitale per intervenire, nel suo funzionamento, sulle grandezze elettriche. Il collegamento può essere realizzato utilizzando un ampio e diversificato numero di mezzi fisici di comunicazione, che utilizzano differenti tecnologie elettroniche che nel corso degli ultimi 30 anni sono state sviluppate ed immesse sul mercato per permettere e garantire lo scambio di informazioni:

- collegamenti cablati
- collegamenti wireless
- collegamenti in powerline (onde convogliate)
- utilizzo delle reti IP

L'interazione tra le Applicazioni oltre che tra queste e l'utente, ha le basi nello scambio di informazioni, che può avvenire via cavo o wireless, a seconda delle circostanze operative e dalle condizioni applicative. In un'epoca che vede una grande diffusione di sistemi che comunicano in modalità wireless, ci si può domandare fino a che punto sia oggi opportuno realizzare reti cablate. In realtà devono essere presi in considerazione tutti i vantaggi di questa soluzione costruttiva e nel contempo non sottovalutare i limiti che inevitabilmente una comunicazione wireless può introdurre.

Ad esempio:

- le comunicazioni wireless presentano limiti di distanza tra i dispositivi molto più restrittivi rispetto alle reti cablate e sono condizionate da fattori ambientali e dagli elementi costruttivi dell'edificio che possono ulteriormente limitare l'area di copertura del segnale;
- i dispositivi wireless, essendo in genere alimentati a batterie, sono concepiti per minimizzare i consumi di energia e salvaguardare l'autonomia dei dispositivi. Questo costringe i costruttori a realizzare componenti con una semplice e rudimentale, quando presente, interfaccia verso l'utente (ad esempio display) e ad alternare stati di funzionamento a stati di inattività;
- la comunicazione wireless, non essendo confinata all'interno di cablaggi, è potenzialmente intercettabile ed accessibile, e pertanto introduce problematiche di sicurezza e di privacy verso potenziali accessi fraudolenti non autorizzati;
- molti dispositivi, per il loro intrinseco funzionamento, necessitano comunque di essere connessi alla rete elettrica (ad esempio attuatori o carichi) e pertanto richiedono comunque la posa di canalizzazioni e collegamenti elettrici, riducendo pertanto il vantaggio dell'assenza di cablaggio tipico dei sistemi wireless.

Ad oggi però, vista la maggiore tendenza a ristrutturare edifici già esistenti, piuttosto che a costruire nuove strutture (e quindi già predisposte con connessioni wired), le applicazioni per migliorare l'efficienza energetica, il controllo e l'automazione degli impianti dell'edificio (BEMS ed BACS) sono implementate prevalentemente con tecnologie basate sulla connettività wireless, che meglio si prestano, per la flessibilità e la bassa invasività nell'impiego, all'installazione in strutture preesistenti.

Le soluzioni wireless utilizzano la radiofrequenza (RF) come mezzo fisico di comunicazione. I dispositivi RF sono alimentati prevalentemente a batteria e possono essere posizionati dovunque all'interno dell'edificio oppure utilizzati come dispositivi mobili. Esistono diverse tecnologie wireless classificabili in funzione della frequenza utilizzata, della distanza di comunicazione, del throughput (capacità di comunicazione) e del costo.

Nella classificazione della distanza di comunicazione si possono distinguere le reti PAN (Private Area Network), LAN (Local Area Network) e WLAN (Wireless Local Area Network) che hanno la capacità di coprire una distanza massima di 100 metri, mentre le reti MAN (Metropolitan Area Network) e WAN (Wide Area Network) raggiungono una distanza massima di 30-50 km.

Nelle reti PAN/LAN si inquadrano le tecnologie Wi-Fi, Bluetooth e Sub GHz; Wi-Fi e Bluetooth sono degli standard (con frequenze da 2.4 a 5GHz) e quindi interoperabili con i dispositivi che aderiscono al medesimo standard, mentre, nel caso di soluzioni Sub GHz, un protocollo utilizzato è il 6LoWPAN, dove è possibile identificare ogni nodo intelligente utilizzando un indirizzo IPv6. La distanza di connessione viene incrementata, rispetto ad una connessione punto-punto, grazie alla topologia "mesh", dove ogni nodo può ripetere il messaggio del nodo adiacente, propagandolo.

Il Bluetooth SIG (Special Interest Group) ha rilasciato le specifiche per il Bluetooth Low Energy Mesh Network, per implementare una rete con topologia mesh, utilizzando lo standard Bluetooth Low Energy; questo standard definisce come creare, controllare e monitorare una rete BLE ed ogni nodo della rete utilizzando uno Smart Phone.

Nelle reti MAN/WAN le tecnologie più rilevanti oggi sono LoRa, Sigfox e le nuove varianti dello standard LTE, ovvero LTE-M e NB-IoT. LoRa e Sigfox sono tecnologie wireless, sub 1-GHz, che adottano un business model differente ma entrambe sono capaci di comunicare a distanze elevate con un basso consumo di energia.

La trasmissione di informazioni mediante onde convogliate è una tecnologia consolidata sebbene poco diffusa. Consiste nell'"iniettare" segnali ad alta frequenza su un mezzo di trasporto costituito dalla rete elettrica (ovvero a frequenze diverse da quelle della rete elettrica che tipicamente sono di 50-60Hz), sfruttando così il cablaggio elettrico esistente. Questa tecnologia è denominata PLC o Power Line Communication. L'uso di questo mezzo di comunicazione, come si può immaginare, è vantaggioso per tutti quei dispositivi che sono, per loro natura, già connessi alla rete elettrica.

Quando si utilizza questa tecnologia di comunicazione occorre tener conto di alcuni aspetti:

- in una rete elettrica sono presenti organi di sezionamento elettrico manuali o automatici il cui intervento, interrompendo la rete elettrica, blocca conseguentemente anche la trasmissione del segnale di comunicazione.
- nelle reti elettriche, anche in ambito residenziale, sono oramai diffusi utilizzatori costruiti con componenti elettronici che possono alterare la forma d'onda del sistema elettrico di alimentazione, introducendo componenti elettriche in alta frequenza, note come "armoniche". Questo fenomeno può generare "rumore" elettromagnetico che può, in alcuni casi, disturbare le comunicazioni PLC rendendo più complesso ed oneroso il sistema di codifica e decodifica delle informazioni.

Queste informazioni devono essere scambiate in un linguaggio comune: il "protocollo di comunicazione".

Panoramica sui protocolli di comunicazione e loro classificazione

I sistemi di automazione di edificio nacquero in gran parte tra la fine degli anni '80 e l'inizio degli anni '90 in Europa e negli Stati Uniti d'America. All'inizio vennero tutti creati dai singoli costruttori elettronici ed elettrotecnici, ma ben presto si assistette ad un processo di convergenza internazionale finalizzato alla creazione di uno standard comune e riconosciuto dalle norme tecniche. Questo processo è giunto fino ai nostri giorni, identificando sul mercato alcuni protocolli e sistemi ormai considerati standard in tutto il mondo.

Oggi il panorama dei sistemi di automazione di edificio contempla alcuni principali standard, con diffusione mondiale ed aperti: KNX, BACNET, M-Bus.

KNX: sviluppato agli inizi degli anni '90 sotto il nome di EIB (European Installation Bus) in Germania, assunse il nome attuale di KNX (Konnex) quando le principali organizzazioni allora presenti nel settore dell'automazione di edificio decisero di dare inizio al progetto di uno standard comune che potesse unire sinergicamente le singole risorse. Oggi dopo 30 anni è diventato il protocollo di comunicazione standard aperto più diffuso al mondo nei sistemi di home e building automation. Come mezzo di comunicazione può utilizzare: quello cablato, quello wireless, la powerline e la rete IP.

BACNET: nasce anch'esso all'inizio degli anni '90 negli USA nel mondo dell'HVAC come protocollo di integrazione tra sistemi. BACNET (Building Automation and Control NETWORKS) oggi continua ad essere diffuso in Europa soprattutto come protocollo di integrazione tra sottosistemi e non di campo. Come mezzo di comunicazione utilizza prevalentemente la rete IP.

M-Bus (Meter Bus): è un protocollo che nasce per la lettura di contatori di ogni genere in Germania, nell'Università di Paderborn. Diventa uno standard europeo nell'ambito della contabilizzazione di energia. Può utilizzare due canali di comunicazione: quello cablato e quello wireless.

Dovendo descrivere, senza scendere nel dettaglio tecnico, i sistemi di automazione attualmente presenti sul mercato, possiamo definire delle macro-categorie di sistemi di automazione che si differenziano per le caratteristiche dei sistemi di comunicazione, i relativi protocolli utilizzati e per l'architettura che li caratterizza.

Una prima classificazione individua i sistemi in relazione a come viene gestita l'intelligenza del dispositivo. Troviamo sistemi:

- ad intelligenza distribuita

Il cui funzionamento è basato su un'intelligenza distribuita nei singoli dispositivi che, oltre ad assicurare interoperabilità, caratterizza l'installazione con un'elevata affidabilità. L'assenza di un dispositivo "centrale" che è deputato a coordinare e a far funzionare i dispositivi rende impossibili le più comuni cause di malfunzionamento. Se un dispositivo si guasta, viene meno esclusivamente la funzione che quello specifico componente svolgeva.

- ad intelligenza centralizzata

Sistemi il cui funzionamento dipende da una intelligenza centrale. Questi sistemi trovano impiego nell'automazione industriale di processo mentre sono fortemente sconsigliati nelle applicazioni legate all'automazione dell'edificio, a vantaggio dei sistemi ad intelligenza distribuita.

Una ulteriore macro-divisione che è venuta a crearsi sul mercato riguarda tecnologie e protocolli impiegati. Esistono sistemi:

- con tecnologia proprietaria.

Si tratta di sistemi sviluppati, sia per la parte relativa alla comunicazione fisica che per quella associata ai protocolli di comunicazione, da singole aziende che ne curano ricerca e sviluppo e l'evoluzione degli stessi. Sono sistemi per loro natura non interoperabili a meno dell'utilizzo di appositi gateway di comunicazione.

- con tecnologia standard aperta

I vantaggi dello standard possono essere così sintetizzati:

- interoperabilità tra diversi dispositivi e tra funzioni indipendentemente dal costruttore;
- certificazione dei prodotti da parte terza: i prodotti vengono autorizzati da appositi laboratori accreditati a riportare un marchio che ne identifica la piena compatibilità della parte elettrica e/o del protocollo con lo standard di riferimento e quindi la interoperabilità funzionale del dispositivo;
- riconoscimento internazionale: le conoscenze e competenze tecniche che l'installatore o l'integratore di sistema acquisiscono nella realizzazione di sistemi hanno valore internazionale;

- scalabilità: il sistema può crescere nel tempo aggiungendo funzioni o potenziando funzioni esistenti con nuovi prodotti immessi sul mercato, garantendo la retro-compatibilità. Lo standard conferisce alla tecnologia un valore che permane nel tempo, perché non legato al singolo costruttore.

Il Gateway un aggregatore che connette il campo al Cloud

Fintanto che i sistemi di domotica e di building automation sono stati gestiti esclusivamente in una logica di “campo”, non si è sentita l’esigenza di sviluppare apparecchiature con funzione di gateway, ovvero di ponte tra il mondo reale ed il mondo digitale della rete Internet. Questa esigenza nasce in seguito alla diffusione e all’affermazione di standard aperti e al crescente riconoscimento del valore di una maggiore integrazione dei sistemi tecnologici all’interno dell’edificio.

Nel mercato sono pertanto nate aziende e figure professionali destinate a impegnarsi con il loro know-how in questa attività di integrazione: i “system integrator”. Gli aggregatori consentono ai system integrator di poter mettere in comunicazione sistemi che per loro natura utilizzano mezzi trasmissivi e protocolli di comunicazione differenti, attraverso una “traduzione” bidirezionale, elettrica e semantica delle informazioni che transitano da un sistema ad un altro.

Oggi con l’avvento delle tecnologie che vanno sotto la nota sigla di IoT (Internet of Things), gli aggregatori si sono ulteriormente evoluti diventando IoT gateway, ovvero non solo aggregatori ma anche instradatori dei dati verso il Cloud, così da offrire la possibilità di connettere l’edificio ai sistemi informatici in Cloud e dando anche la possibilità, laddove richiesto, di pre-elaborare a livello di IoT gateway i dati raccolti dai sensori prima di essere trasferiti.

Nasce così una nuova modalità di integrazione degli impianti. Questi dati possono essere trattati ed elaborati da applicativi installati nel Cloud o nei dispositivi mobili quali smartphone e tablet per poi inviare di ritorno comandi di attuazione ai dispositivi stessi o ad altri. Questa opportunità tecnologica offre la possibilità di poter creare integrazioni tra sistemi in campo attraverso applicativi in Cloud o attraverso le App. Questa modalità di controllo non è da intendersi sostitutiva di quella effettuata “in campo”, ma è solo una opportunità in più che la tecnologia mette a disposizione degli integratori di sistema nell’attività di integrazione degli impianti.

Le informazioni da trattare ed analizzare infatti possono essere di due tipi:

- critiche e con la necessità di essere scambiate tra dispositivi in “Real time”, ovvero necessariamente entro intervalli di tempo ben determinati e molto brevi. I dati che danno origine a questo tipo di informazione devono necessariamente essere elaborati localmente e alcuni gateway consentono l’installazione di applicativi locali da usare a tale scopo. I tempi di latenza dovuti al canale di trasmissione dal campo verso il Cloud, alla risposta nella elaborazione degli applicativi ed alla ritrasmissione verso il dispositivo destinatario non sono “determinabili” temporalmente con precisione e pertanto non sono compatibili con funzioni critiche. Tecnicamente gli applicativi che si eseguono lato Cloud sono da considerarsi “non deterministici”;

- non critiche: informazioni per le quali i tempi di latenza sopra descritti sono compatibili con la funzione dell'informazione stessa. I dati relativi a queste informazioni possono essere inviati a sistemi Cloud ed essere elaborati da applicativi su questi installati.

Pertanto, sono nati, a seconda delle due esigenze sopra descritte, differenti tipi di gateway di aggregazione: gli IoT gateway con capacità di elaborazione locale e programmabili da remoto e gli IoT gateway che hanno la sola funzione di serializzare i dati ed inviarli al Cloud per le successive elaborazioni. Gli scopi sono gli stessi ma le modalità sono diverse:

- raccolta e scambio dei dati con il Cloud e localmente con capacità locali di elaborazione, anche complessa, per impieghi critici e real-time;
- raccolta e scambio dei dati con il Cloud e localmente tra sistemi per integrazione funzionale o condivisione nel caso non sia necessario effettuare delle azioni real-time.

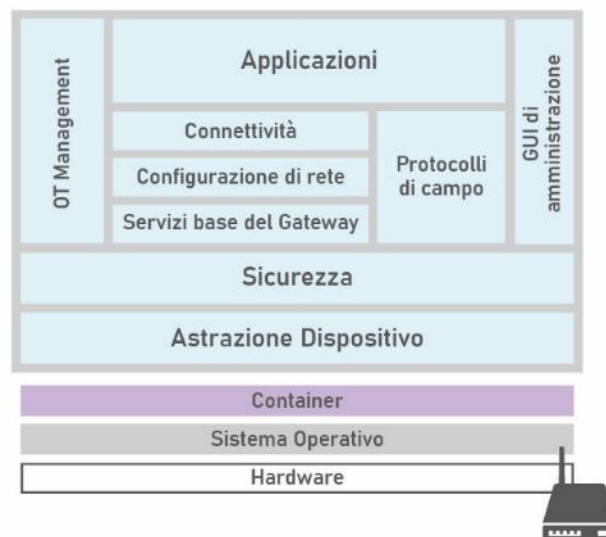


Figura 20: Componenti funzionali di un gateway IoT

Dagli IoT gateway in campo ai software gateway nel Cloud

Ci sono due macro-tipologie di integrazione di sistemi IoT eterogenei: un metodo è quello, come si è descritto nel paragrafo precedente, di integrare questi sistemi “in campo”, attraverso un IoT gateway hardware; un altro è quello di farlo mediante dei software gateway residenti nel Cloud o con apposite applicazioni che accedono ai dati dei rispettivi sistemi IoT tramite chiamate REST.

I gateway hardware sono normalmente dei dispositivi computerizzati di complessità crescente e che possono essere dotati di funzioni di programmazione crescenti, ovvero possono essere dotati solo di un apposito firmware con funzioni e caratteristiche predeterminate o, nelle versioni più evolute, sono dotati di un software framework che ne consente la programmazione da remoto e la possibilità di eseguire in maniera concorrente diversi applicativi lato gateway.

Esiste come detto anche un ulteriore modo di integrazione tra sistemi, che avviene a livello logico nel Cloud attraverso “gateway” Cloud-to-Cloud, ovvero tramite applicativi software che possibilmente fanno uso di chiamate REST. Per ogni sistema da integrare si parte da uno specifico Gateway che unisce il campo con il Cloud. Questi sono invece dispositivi che servono a trasferire le informazioni dei sensori/attuatori o da specifici bus di campo verso un Cloud e astraendone il formato. L’informazione che raggiunge il Cloud è pertanto depurata dai dettagli tecnologici del sistema presente in campo. Una volta che i dati sono sui rispettivi Cloud, il processo di integrazione tra sistemi diversi può essere effettuato da applicazioni software che agiscono sui dati che sono a questo punto svincolati dalla tecnologia di campo utilizzata. Grazie appunto alle nuove metodiche di sviluppo basate su chiamate REST, le applicazioni richiedono tempi di sviluppo e aggiornamento molto brevi e possono essere realizzate da personale tecnico con competenze informatiche che non deve necessariamente conoscere la tecnologia dei protocolli utilizzati in campo. Il formato tecnologico attraverso cui queste informazioni vengono rese disponibili per elaborazioni su sistemi Cloud va sotto il nome di API (Application Programming Interface).

Piattaforma di raccolta e di fruizione dei dati su Cloud tramite API

In precedenza, si è sottolineato la necessità di costruire l’architettura a partire da strati debolmente accoppiati così da disaccoppiare l’acquisizione dati dall’elaborazione degli stessi. Visto che la concatenazione dei dati IoT può essere schematizzata in tre fasi - acquisizione, trasmissione ed elaborazione - la soluzione architetturale più semplice è quella di dividere il problema in tre macro sottosistemi: il sottosistema di campo con sensori/attuatori e IoT Gateway che si interfaccia con la rete TCP/IP al resto dell’architettura, il sottosistema di comunicazione con la Piattaforma nel Cloud (public/private/on-premise) con interfaccia TCP/IP verso i gateway e interfacce API di tipo REST verso i programmi e per finire il sottosistema IT con l’ecosistema dei programmi, siano essi programmi che girano nei server, nei computer locali o nei dispositivi mobili come le App. Visto che del Gateway ci siamo occupati in precedenza qui ci occuperemo delle funzionalità della Piattaforma IoT. Questo componente funziona come uno strato di integrazione. La Piattaforma fornisce agli utenti una combinazione di servizi Cloud, collettivamente chiamati servizi di piattaforma di integrazione, per sviluppare e per eseguire e gestire i flussi di dati provenienti dai dispositivi IoT tramite i gateway. La Piattaforma offre anche altre funzionalità aggiuntive per integrarsi all’ambiente IT (Information Technology) consentendo all’infrastruttura di campo, ovvero le Operational Technologies (OT), in questo caso i sensori e attuatori negli edifici, collegati ai gateway, di essere visti come un’estensione dell’ambiente IT senza tutte le complessità specifiche d’interfacciamento e accesso a sensori e attuatori stessi.

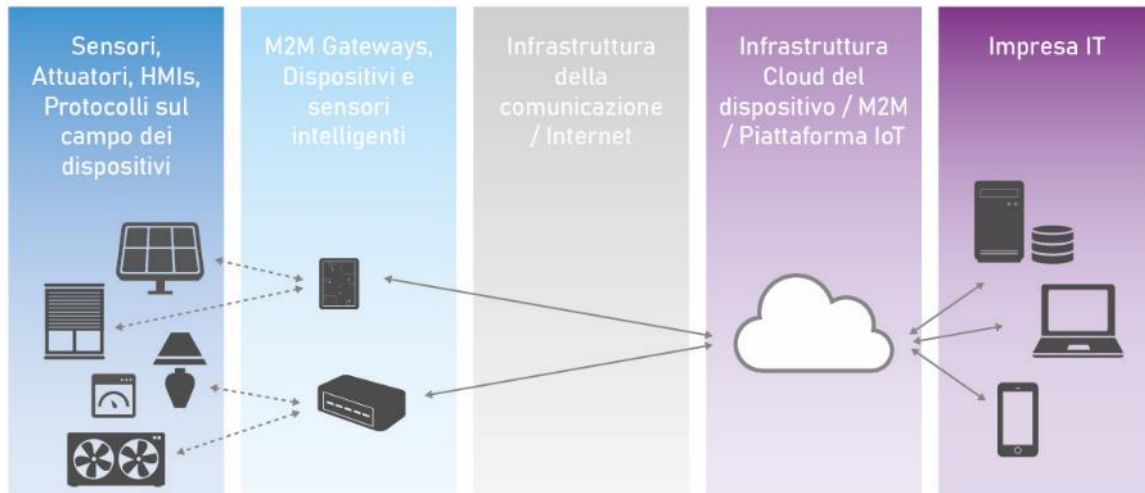


Figura 21: Suddivisione in sottoinsiemi di una architettura IoT

Una infrastruttura Internet of Things, che crea un ponte tra il mondo complesso e frammentato di sensori e attuatori e il mondo delle applicazioni IT, deve essere quanto più agnostica e generale possibile ed essere preferibilmente fruibile come un servizio, da cui il nome Platform as a Service (PaaS). I servizi minimi che una piattaforma IoT deve fornire sono quelli di base per poter gestire le fasi di:

- autenticazione e installazione dei gateway IoT inclusa la loro configurazione ed il ciclo di vita;
- il trasporto, la sicurezza e la distribuzione dei dati IoT;
- le funzioni di autenticazione, autorizzazione e accesso ai dati da parte degli utenti;
- le funzioni di autorizzazione e accesso ai dati da parte delle applicazioni.

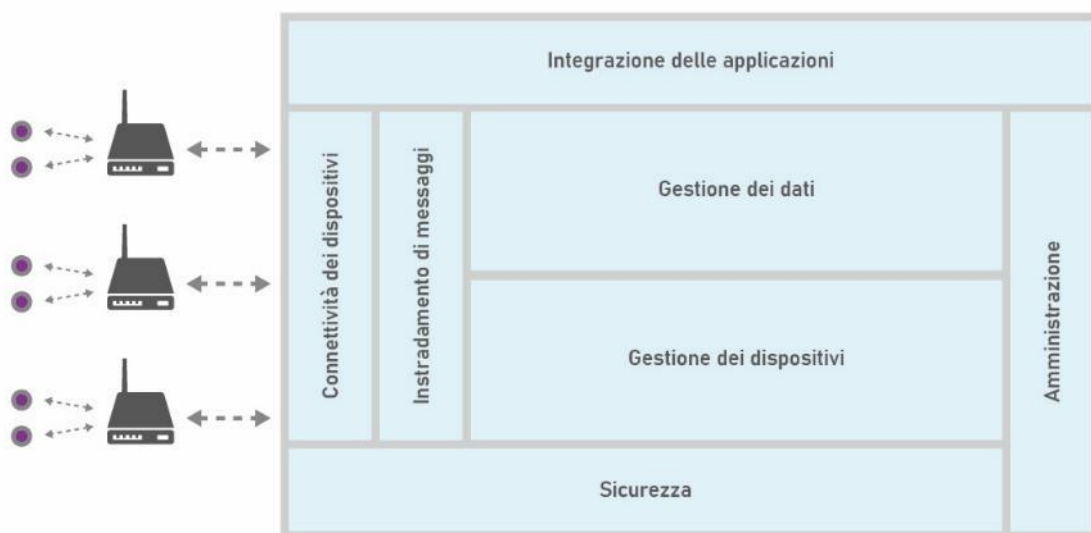


Figura 22: Componenti funzionali di una piattaforma IoT

Da quanto sopra detto si possono identificare due flussi con cui la piattaforma ha a che fare: il flusso dei dati scambiati con i gateway e il flusso di dati scambiati con le applicazioni.

Il flusso dei dati scambiati con i gateway a sua volta può essere diviso in due flussi: il flusso dei dati scambiati con le cose e il flusso di dati generati dalle funzioni di gestione (identità del dispositivo,

integrità SW, stato di salute, aggiornamento SW, impostazioni di tempo reale, etc.). Il flusso di dati delle “Cose” impatta sia le applicazioni che la tipologia di servizi che si vogliono erogare mentre i flussi dati per la gestione remota dei gateway impatta principalmente sui costi di messa in esercizio degli stessi e sui costi ricorrenti di gestione dell’infrastruttura IoT. Pertanto, oltre a garantire una facile scrittura delle App, una piattaforma IoT deve garantire una facile installazione, gestione e manutenzione dei gateway IoT o dei sensori/attuatori intelligenti.

Building: Chi genera i dati e a chi interessano

L'estensione del concetto di Digital Twin al Building: una possibile evoluzione del BIM?

Navigare nel panorama tecnologico nella maggior parte dei settori a volte può rivelarsi un incubo. Il gergo può essere infinito e, con il ritmo del cambiamento tecnologico che accelera ogni anno, non sorprende che le industrie siano lente a definire e articolare le migliori pratiche. In uno scenario indubbiamente evolutivo, il mondo delle costruzioni continua purtroppo a mantenere il primato negativo del settore industriale meno recettivo all'innovazione tecnologica e alla trasformazione digitale. Tuttavia, la crescente attenzione al BIM – Building Information Modelling - sta interessando negli ultimi anni tutti i principali attori di una filiera complessa, qual è quella delle costruzioni, consolidando in tutte le parti in gioco la consapevolezza dell'importanza della modellizzazione dei dati in ciascuna delle fasi del processo, fino al risultato finale, che è appunto l'edificio.

Come introdotto precedentemente in questo libro, il paradigma del Digital Twin sta rapidamente diventando il punto di partenza per la creazione di solidi modelli di dati su diversi settori, come l'industria, l'automotive e molti altri. Ai più non sfuggiranno le somiglianze chiave tra ciò che è ora chiamato un gemello digitale di un ambiente costruito e i software BIM, Building Information Modelling.

Comprensibilmente c'è stata una certa confusione, con riferimento all'Edificio, su come differenziare queste due importanti tecnologie. La confusione in gran parte si riduce all'enfasi del software BIM sullo spazio fisico rappresentato digitalmente e la definizione iniziale di Digital Twin, una replica digitale di un oggetto o spazio fisico. Per cominciare ad analizzare le differenze chiave tra Digital Twin e BIM, facciamo riferimento ad un interessante articolo³⁴, pubblicato nel 2019 sul portale IoT for all.

Cominciamo con il BIM. Come il concetto di Digital Twin, esiste anch'esso da diversi anni. Nato come software negli anni '70 attraverso un progetto di R&D, annovera tra i primi ricercatori Chuck Eastman che iniziò, tra gli altri, ad usare il termine "Sistema di descrizione dell'edificio" prima che diventasse BIM. Analogamente al Digital Twin, anche il BIM non ha attecchito per alcuni decenni, finché realtà del calibro di Autodesk, Bentley Systems e altri hanno iniziato a diffonderlo nei primi anni 2000.

Le ragioni che hanno dato origine al BIM restano ancora valide. I padri fondatori del BIM avevano ipotizzato che un tale sistema sarebbe stato importante per gli appaltatori di grandi progetti, sia come modello visivo che quantitativo della costruzione utile soprattutto per programmare temporalmente e quantitativamente l'approvvigionamento dei materiali.

Ancora oggi, i principali fornitori di software BIM si rivolgono agli architetti, ingegneri e appaltatori spiegando i vantaggi economici che derivano dal poter disporre di un modello digitale 3D

³⁴ <https://www.iotforall.com/digital-twin-vs-bim/>

dell'Edificio. Questo modello semplifica la collaborazione tra le parti coinvolte nel processo e la ricalibrazione del progetto durante le sue fasi, con evidenti vantaggi derivanti da un maggior controllo del rischio, dovuto alla potenziale riduzione degli errori e a una migliore gestione dei tempi e del budget. Quindi BIM indubbiamente simile al Digital Twin, ma ne differisce per alcuni aspetti chiave.

Il BIM è concepito per ottimizzare le fasi di progettazione e costruzione, non attualmente per intervenire su operazioni successive nell'edificio /o per le attività di manutenzione. In altri termini, a differenza di un effettivo gemello digitale dell'edificio, il modello di informazioni fisiche BIM è attualmente efficace per gli edifici in costruzione, non per quelli occupati e utilizzati quotidianamente.

Ed è qui che entra in gioco il ruolo del Digital Twin, in grado di restituire una rappresentazione real-time dell'edificio, dei sistemi e sottosistemi che lo compongono, del loro stato e di come il loro funzionamento è influenzato dalla presenza e comportamento degli occupanti. Se finora il BIM, in quanto sistema di supporto alla sola progettazione, si pone come uno tra i diversi aggregatori di dati per un modello Digital Twin dell'edificio, una sua evoluzione come software di gestione completa del ciclo di vita dell'edificio lo porrebbe come elemento cardine per determinare una reale transizione digitale delle costruzioni ed un inquadramento delle stesse in una logica IoT.

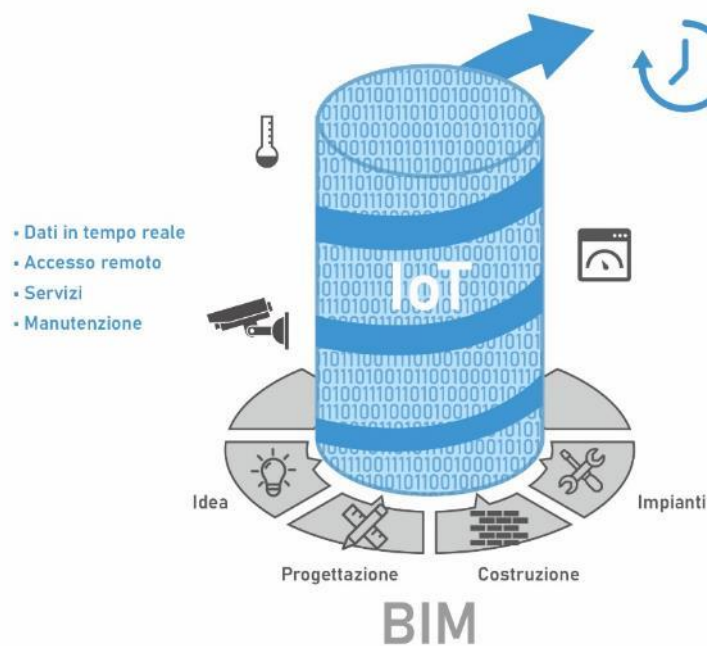


Figura 23: BIM vs IoT

Il concetto di Servizio e di Applicazione per diverse tipologie di edifici

Ai fini del presente capitolo il concetto di Servizio viene inteso come una soluzione tecnologica, relativa ad uno o più degli impianti di edificio, che gode di autonomia funzionale (non dipende da altri Servizi per funzionare) e che è in grado di ricevere informazioni (input) per governare il proprio funzionamento e di generare informazioni (output) relative allo stesso.

Il concetto di Applicazione si riferisce invece alla soluzione tecnologica (generalmente software) in grado di operare in modo trasversale sui dati forniti dai diversi Servizi per realizzare nuove funzionalità e quindi trarre maggior valore dai dati stessi. Ovviamente il concetto di Applicazione è abitualmente utilizzato anche per i dati di un singolo Servizio, ma in questa trattazione questa accezione è volutamente lasciata in secondo piano per dare maggiore enfasi al valore dell'integrazione.

È utile premettere che i Servizi che generano dati all'interno di un edificio possono essere estremamente diversificati, anche in relazione alle diverse categorie di edifici. Pur limitando l'analisi agli edifici del settore terziario e residenziale, questa diversificazione esiste comunque: si pensi, ad esempio, alle differenze che possono esserci fra i Servizi all'interno di una struttura ospedaliera e quelli all'interno di un centro commerciale o di un complesso di condomini al centro di una città, collegati ad un sistema di teleriscaldamento.

In questo senso il presente capitolo si sviluppa con una prima analisi che riguarda gli aspetti comuni alla maggior parte degli edifici, mentre nei paragrafi successivi viene posta l'attenzione sugli aspetti relativi a categorie specifiche di edifici, caratterizzati dalle attività che si svolgono all'interno degli stessi.

Questo approccio consente, fra l'altro, di distinguere meglio i **Servizi "verticali"** (specifici del singolo segmento) da quelli **"orizzontali"** (comuni alle diverse tipologie di edifici), ma non deve far perdere di vista il fatto che una componente imprescindibile dell'approccio IoT è proprio legata all'interoperabilità dei Servizi, che quindi devono essere considerati nella loro globalità. Per non perdere di vista questo obiettivo, all'interno della disamina dei Servizi "verticali", si cercherà di sottolineare proprio le interazioni possibili con i Servizi "orizzontali".

Da non trascurare, oltre agli aspetti tecnologici e per avere una visione completa dell'impatto di queste nuove tecnologie, la **User Experience** e cioè il punto di vista degli utenti: qual è l'impatto sociale delle nuove Applicazioni? Molto spesso il successo o il fallimento di nuovi approcci tecnologici derivano proprio dal grado di accettazione/gradimento da parte degli utilizzatori e quindi questo aspetto va sempre tenuto nella massima considerazione.

Servizi "orizzontali" o comuni ai diversi settori

Nel trattare i Servizi comuni ai diversi settori è utile premettere alcune considerazioni circa la trasformazione in corso della rete di distribuzione elettrica, anche in conseguenza della continua crescita della generazione di energia di tipo rinnovabile. Il nuovo modello di generazione distribuita che si sta affermando richiede sempre maggiore "intelligenza" e capacità di operare in maniera attiva sia da parte dei sistemi di generazione, sia della rete, sia dei nodi utilizzatori, modulando quindi con sempre maggiore frequenza e flessibilità, produzione, trasmissione e distribuzione di energia.

Se opportunamente modulata, con soluzioni “light” per le realtà di più piccole dimensioni e soluzioni “heavy” nel caso di operatori che possano ragionare in ottica multi-impianto, la scelta di soluzioni digitali per la gestione della generazione di energia appare una scelta vincente, non soltanto per il proprietario o gestore dell’impianto, che ne ottiene un beneficio economico diretto, ma anche per il sistema elettrico nel suo complesso, che guadagna in termini di affidabilità e flessibilità nella fase di generazione.

Nell’analizzare i Servizi comuni a tutte le tipologie di edifici è utile raggrupparli in due principali categorie, che corrispondono anche a due acronimi spesso utilizzati nella letteratura e nella normativa che tratta il settore:

- **BEMS Building Energy Management System.** Rientrano in questa categoria i Servizi generalmente rivolti ad analizzare la performance energetica dell’edificio e la sua evoluzione/previsione. Spesso, fra i dati raccolti dal BEMS, ci sono quelli relativi al funzionamento di Servizi controllati dal BACS.
- **BACS Building Automation and Control System.** Si tratta di Servizi rivolti al controllo e all’automazione del funzionamento degli impianti/sistemi tecnici di edificio. Le funzioni di automazione possono essere molto sofisticate, prevedendo algoritmi di regolazione/ottimizzazione multifattoriali che richiedono anche scambio di informazioni fra Servizi diversi.

Servizi che generano dati → BEMS

- **Monitoraggio dei consumi elettrici.** All’interno di questo Servizio sono comprese tutte le misure dei consumi elettrici, che vanno da quelle realizzate leggendo i misuratori fiscali forniti dai distributori (con tecnologie e periodicità diverse, utilizzando sia apparecchiature di lettura realizzate ad hoc, sia interfacce messe a disposizione dai misuratori stessi) fino a quelle realizzate aggiungendo apparecchiature di misura specifiche. Vanno sempre più diffondendosi componenti dell’impianto elettrico collegabili che, in modo nativo, rendono disponibili sia informazioni relative al loro funzionamento (stato di funzionamento, allarmi, richieste di manutenzione), sia informazioni relative alle componenti gestite (misure di tensione, corrente, potenza, qualità dell’energia, ecc.).

È utile ricordare che all’interno di questo Servizio vengono talvolta considerate le cosiddette “misure virtuali” realizzate tramite calcoli su grandezze conosciute. Per esempio, sapendo che a valle di un interruttore è presente un carico fisso da 1kW (una linea di illuminazione non regolabile) è possibile calcolare i consumi monitorando il tempo in cui l’interruttore stesso rimane chiuso.

- **Monitoraggio dei consumi termici.** Trend analoghi si riscontrano per i Servizi di monitoraggio dei consumi termici, dove tuttavia la capillarità di rilevazione degli stessi è minore (anche per i costi leggermente superiori delle relative apparecchiature). In questo caso, come nel precedente, apparecchi generatori e utilizzatori forniscono informazioni relative al loro stato di funzionamento e all’energia generata/utilizzata. È da segnalare, per questo Servizio e in ambito condominiale, la sempre maggiore diffusione (anche per il relativo obbligo normativo a livello europeo) di sistemi per la ripartizione dei consumi di

edificio sulla base di parametri di utilizzo rilevati all'interno dei singoli appartamenti e dei singoli corpi riscaldanti (contabilizzazione indiretta).

- **Monitoraggio di altri consumi.** Attraverso l'uso di strumenti di misura ad hoc o l'interfacciamento di misuratori fiscali vengono altresì rilevati i consumi di gas, di acqua e acqua calda sanitaria.
- **Monitoraggio delle condizioni di funzionamento dell'edificio.** Si tratta di un Servizio spesso sovrapposto (ove esiste) con le funzioni del BACS. Vengono raccolte, ai fini della valutazione della prestazione energetica dell'edificio, parametri quali le temperature interne/esterne, livelli di umidità e di CO₂, stati e grandezze relative ai funzionamenti di apparati.

Servizi che generano dati → BACS

- **Automazione e controllo dei sistemi tecnici elettrici degli edifici** (es. distribuzione elettrica, illuminazione, oscuranti, scale mobili, ascensori, storage, produzione da fotovoltaico, ecc.). Implementano questo Servizio sensori, attuatori, moduli di ingresso/uscita e controllori che consentono di acquisire gli stati e regolare il funzionamento degli impianti e delle relative apparecchiature. A titolo di esempio possono essere citate le funzioni di regolazione dell'illuminazione di un ambiente in base a parametri quali il tipo di attività, la presenza di persone, l'apporto di luminosità esterna, l'orario, ecc.
- **Automazione e controllo dei sistemi termotecnici e meccanici degli edifici** (es. HVAC, ovvero Heating, Ventilation and Air Conditioning). Implementano questo Servizio sensori, attuatori, moduli di ingresso/uscita e controllori che consentono di acquisire gli stati e regolare il funzionamento degli impianti e delle relative apparecchiature. A titolo di esempio possono essere citate le funzioni di regolazione della temperatura di un ambiente tramite il comando di fan-coil sulla base di parametri quali il tipo di attività, la presenza di persone, l'orario, ecc.
- **Sicurezza delle cose** (es. controllo accessi, antintrusione, videosorveglianza)
- **Sicurezza delle persone** (es. rivelazione fumi, rivelazione gas, rivelazione di allagamento, evacuazione guidata, illuminazione emergenza).

Per ciascuno di questi Servizi è in atto, da tempo, un processo tecnologico per cui sono in costante aumento i componenti collegabili in modo nativo ed in grado di trasferire informazioni circa il proprio stato e la funzione a cui sono preposti. A volte l'intero Servizio è fornito come un unico sistema integrato con il quale è possibile scambiare dati tramite opportuni protocolli di comunicazione (è il caso tipico, ad esempio, dei sistemi di antintrusione per i quali esistono delle norme prescrittive piuttosto vincolanti).

A chi interessano i dati e i relativi Servizi

Come evidenziato nei punti precedenti, dai sistemi tecnici di edificio (cd. Servizi orizzontali BEMS+BACS) vengono generate e/o trattate una quantità innumerevole di informazioni. A livello di singolo Servizio questi dati sono utilizzati per l'implementazione delle logiche alla base del funzionamento del Servizio stesso, e quindi per governare e ottimizzare il funzionamento delle apparecchiature controllate.

Il nuovo scenario IoT prevede che tutte le informazioni generate dai diversi Servizi siano rese disponibili per la realizzazione di una nuova classe di Applicazioni software (di seguito solo Applicazioni) che, operando in modo trasversale sulle stesse, siano in grado di fornire nuovi

strumenti decisionali agli stakeholder di settore. Di seguito sono citati alcuni esempi di queste Applicazioni, con la consapevolezza che, operando su entità astratte quali i dati, e potendo accedere anche ad informazioni rese disponibili da Servizi esterni all'edificio (servizi web sui costi dell'energia, servizi web di previsioni metereologiche, interfacce alla rete elettrica per l'implementazione di logiche demand/response, ecc.) le Applicazioni realizzabili siano praticamente infinite. Di seguito ne analizziamo alcune.

Applicazione: determinazione della performance energetica dell'edificio. Si tratta di una Applicazione che unisce i dati di BEMS e BACS, correlando i dati di consumo (raccolti dal BEMS) alle modalità con le quali l'edificio viene utilizzato (desunti dal BACS). Tale correlazione consente di effettuare la normalizzazione dei consumi sulla base delle condizioni di utilizzo e quindi di ottenere indicatori di efficienza che la sola analisi dei consumi non consente, realizzando uno strumento decisionale di grande importanza per l'energy manager.

Applicazione: servizi di manutenzione avanzati. Il monitoraggio degli allarmi tecnici (sensori per incendio, per fumi, allagamenti, malfunzionamenti impianti elettrici e termofluidici) può essere remotizzato presso le strutture che devono garantire i relativi servizi. Analogamente possono essere remotizzate le informazioni relative al funzionamento delle diverse apparecchiature presenti in un edificio, consentendo l'implementazione di funzioni di manutenzione predittiva. A titolo di esempio: i consumi elettrici (BEMS) e i parametri di funzionamento di una UTA, Unità di Trattamento dell'Aria (BACS) possono essere messi in correlazione per determinare lo stato di pulizia dei filtri e programmare un intervento di manutenzione che garantisca il migliore bilanciamento tra i costi di esercizio dell'apparecchiatura e i costi dell'intervento stesso, nel rispetto del comfort per l'utente.

Applicazione: Demand/Response - Prosumer. Il controllo della performance energetica dell'edificio (Esempio 1 di Applicazione) è la base per determinare la previsione dei consumi e quindi essere in grado di negoziare con la rete (Smart Grid) la fornitura di energia. All'interno di questa negoziazione può essere prevista la possibilità, tramite il controllo dei Servizi BACS, di modificare il proprio profilo di consumo nel breve termine per contribuire all'ottimizzazione del funzionamento della rete. Generalmente l'Applicazione Demand/Response è in grado di tenere in conto anche i contributi da FER (Fonti Energia Rinnovabili) presenti all'interno dell'edificio e di implementare le logiche cosiddette Prosumer, che prevedono che l'edificio possa anche fornire energia alla rete e non sono prelevarla. Grazie a questa Applicazione, l'utenza promuove una rete elettrica più verde, stabile ed efficiente.

Applicazione: Il fotovoltaico "interconnesso"

L'opportunità più importante per le FER risiede nella disponibilità sistematica dei dati di produzione e consumo del fotovoltaico. Così facendo l'elettricità solare può acquisire un

valore maggiore perché di fatto maggiormente “programmabile”. Disponendo di informazioni più precise su offerta e domanda di energia, i gestori di rete possono organizzare meglio le proprie decisioni di investimento. D’altra parte, le banche potrebbero ottimizzare i propri modelli di finanziamento se ricevessero automaticamente informazioni sulla disponibilità tecnica degli impianti fotovoltaici. In questa direzione si possono offrire infatti dati con la massima precisione per previsioni affidabili e stime aggiornate sul rendimento fotovoltaico, ovviamente nel rispetto dei massimi standard di sicurezza e privacy.

Gli inverter solari sono inoltre il cuore del sistema fotovoltaico e possono essere considerati a tutti gli effetti i sistemi di controllo, rilevanti per la sicurezza e per il monitoraggio che potrebbe essere integrato nella tecnologia stessa dell’impianto. L’ulteriore aggiunta di apparecchiature per l’accumulo di energia può mettere in grado il sistema di fornire energia non solo in funzione della produzione solare, ma anche in modo asincrono aumentando in modo significativo la flessibilità.

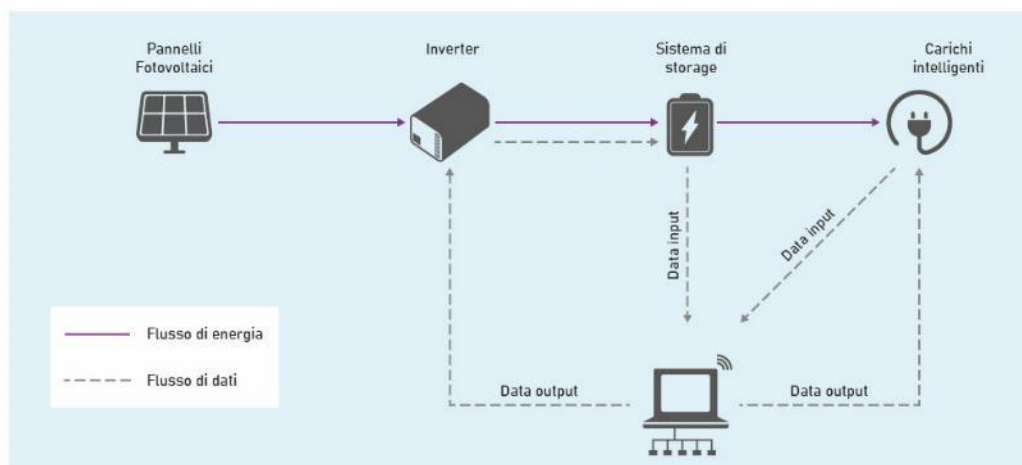


Figura 24: Flussi di dati ed energia

É necessario sottolineare che queste Applicazioni, seppure definite orizzontali, hanno poi delle declinazioni specifiche per ogni segmento di mercato nel quale vengono realizzate. Quindi, per esempio, una Applicazione di Demand/Response realizzata per un condominio avrà alcune caratteristiche diverse da quelle della stessa Applicazione realizzata per un supermercato.

É quindi evidente che la numerosità delle Applicazioni e dei diversi soggetti che possono proporsi per realizzarle (ricordiamo che trattiamo di dati e quindi le attività al riguardo sono tipicamente abituali per tutte le aziende del comparto ICT) apre all’ingresso di nuovi competitors, di nuove figure professionali e di nuovi modelli di business.

Servizi “verticali”

Residenziale: esempi di Servizio, vantaggi e fruibilità

Parlando di residenziale, la casa intelligente o Smart Home si riferisce alla possibilità, o meglio all'opportunità, di collegare tra di loro i diversi Servizi che normalmente fanno parte della infrastruttura tecnologica dell'edificio, per poterne ottimizzare le prestazioni e la gestione, per migliorare il comfort abitativo, per ottimizzare la gestione energetica nell'ottica del risparmio e per incrementare la sicurezza delle cose e delle persone.

I principali Servizi per la casa intelligente già presenti sul mercato si possono riassumere nei seguenti:

- *Climatizzazione/Riscaldamento* – termostati, condizionatori e/o caldaie connesse regolabili in locale o a distanza tramite smartphone o altri dispositivi.
- *Illuminazione* – controlli generali di ON/OFF, gestione scenari sulla base dell'utilizzo o di condizioni predefinite.
- *Motorizzazioni, tapparelle e tende* – controlli generali di ON/OFF, gestione scenari sulla base dell'utilizzo o di condizioni predefinite.
- *Elettrodomestici* – apparecchiature connesse, con accensione/spegnimento da remoto, regolabili in locale o a distanza tramite smartphone o altri dispositivi.
- *Mobilità verticale* - collegamento bidirezionale impianto-servizio di soccorso H24; connessione impianto-edificio, accessi e spostamenti negli edifici, connessione da remoto impianto-impresa di manutenzione, ascensori/piattaforme elevatrici “intelligenti” in servizio H24.
- *Sicurezza* – impianti di allarme, di videosorveglianza e videocitofonia, con possibilità di chiamata in remoto, su smartphone, che in abbinata a serrature intelligenti permettono di aprire al corriere o monitorare l'impianto in caso di allarme.
- *Entertainment* – diffusione sonora, sistemi di home theatre, hub (concentratori) per videogiochi
- *Connettività (telefonia/ADSL/fibra ottica)*

Oggi, oltre ai Servizi tradizionali interconnessi tra di loro, il fenomeno che può aiutare a far decollare le abitazioni intelligenti è senza dubbio la forte e rapida diffusione degli oggetti connessi in un ambiente IoT, spinti non solo dai tradizionali player per i Servizi sopra evidenziati, ma anche da aziende come Apple e Samsung o le stesse Google, Amazon o miriadi di start-up.

Un esempio, diffuso soprattutto a livello internazionale e in particolare negli Stati Uniti, è la crescente diffusione dei cosiddetti **Smart Home speakers**, o **assistenti vocali intelligenti**. Si tratta di veri e propri Hub (concentratori) dotati di altoparlanti, microfoni, display e processori di connessione, che nascono per facilitare l'interazione e il controllo di una pluralità di oggetti intelligenti eterogenei presenti nell'abitazione, da parte dell'utente, con importanti ricadute in termini di interoperabilità e facilità di gestione della propria abitazione. Dispositivi come Amazon

Echo e Google Home stanno spopolando negli USA dove sembra che 35 milioni siano gli esemplari venduti in solo un anno.

L'abitazione dovrà pertanto essere in grado di ricevere questi nuovi oggetti IoT, integrarli nelle funzionalità esistenti e interagire con essi per massimizzare i benefici di uso e di consumo di tutti gli impianti e le funzioni dell'abitazione.

I benefici di queste connessioni tra oggetti e impianti di casa sono anche di tipo economico oltre che relativi al comfort e alla sicurezza. Se ci riferiamo per esempio al riscaldamento, partendo da informazioni strutturali relative all'abitazione considerata (ad esempio la classe energetica, il numero di stanze, l'esposizione, l'area geografica) e da alcune indicazioni sulle abitudini dello specifico utente, è possibile calcolare il risparmio energetico di un'abitazione smart rispetto a una tradizionale. Considerando tre tipologie di nuclei familiari (single, giovani coppie, famiglie con bambini) residenti nel Nord Italia, si può osservare in tutti i casi un risparmio considerevole, compreso tra il 16% (giovani coppie) e il 28% (famiglie con bambini). Alcuni studi hanno simulato che l'adozione diffusa di soluzioni smart per il riscaldamento nella sola area di Milano consentirebbe di ridurre le emissioni di anidride carbonica di oltre 54000 tCO₂ all'anno, con impatti positivi sull'ambiente e con un risparmio annuo di ben 70M€ per i cittadini (pari circa a 100€/famiglia).

Guardando infine all'impatto sociale, le nuove tecnologie influenzeranno positivamente la gestione del nostro tempo, migliorando l'equilibrio tra lavoro e vita privata. Le famiglie di oggi sono diverse rispetto al secolo scorso: i genitori, con ogni probabilità, lavorano entrambi e si dividono gli impegni familiari mentre, quando il genitore è uno solo, le attività sono tutte a suo carico. L'instabilità del mercato del lavoro ha accentuato meccanismi come precariato, contratti a termine, prolungamento dell'età pensionabile e pendolarismo; ne consegue che oltre ad essere impegnatissimi, i genitori sono spesso lontani da casa. Le nuove tecnologie rendono più efficiente l'uso delle risorse e delle attività, sono amiche del nostro tempo e ci consentono di averne di più a disposizione da dedicare alle esigenze personali e familiari.

Esempio 1 → Energy Manager

Nel prossimo futuro non solo gli elettrodomestici, ma tutto il Sistema Casa si svilupperà sulle necessità di intelligenza energetica e il sistema di connessione sarà sempre più efficiente e strutturato. Un nuovo attore diventerà protagonista in casa, l'Energy Manager che si occuperà di sincronizzare le richieste d'utilizzo degli apparecchi con i bisogni dell'utente, in relazione anche ai requisiti della rete elettrica. L'Energy Manager potrà quindi assicurare una gestione intelligente dell'elettricità, che si riflette nella riduzione dell'importo in bolletta, e sarà capace di raccogliere gli input/richieste dell'utente e interagire con tutti i Servizi attivandone le funzioni. Grazie ai sensori che monitorano temperatura, umidità, qualità dell'aria, a centraline meteo o collegamento a siti specializzati, gli impianti termici potranno funzionare nelle migliori condizioni di efficienza, adattando automaticamente la casa alle condizioni esterne più o meno gravose e garantendo in ogni istante il corretto livello di comfort e di salubrità ambientale.

L'attivazione degli elettrodomestici potrà avvenire in base al costo dell'energia nelle diverse fasce orarie, o in base alla disponibilità energetica da fonti rinnovabili o infine per soddisfare una eventuale richiesta di riduzione o spostamento dei consumi da parte della rete elettrica



Figura 25: Relazioni tra elettrodomestici e consumi

Esempio 2 → Gestione coordinata dei Servizi e Scenari personalizzati

È facile immaginare, a titolo di esempio, una situazione in cui si potrà uscire di casa e con un unico comando spegnere tutte le luci, chiudere tutte le tapparelle e inserire l'allarme. Poi nel corso della giornata, direttamente dal proprio posto di lavoro, avviare la lavatrice 'smart' che inizierà il ciclo nel momento di massima produzione dell'impianto fotovoltaico, per minimizzare i consumi energetici. Nel frattempo, sempre da remoto si potrà riconoscere il corriere di Amazon con successiva apertura della porta di casa, con disattivazione temporanea della zona ingresso dell'allarme e consegna del pacco in totale assenza del residente. Nel rientro verso casa, dopo il lavoro, Google potrà geo-localizzare la macchina e settare in modo automatico e trasparente la temperatura di casa, tramite il termostato connesso, a un livello di maggior comfort in relazione alla distanza e alle reali condizioni meteo, per ottimizzare il consumo energetico. Arrivato a casa il residente collegherà la macchina ibrida alla centralina per la ricarica, il cui ciclo verrà ottimizzato in base sempre alle condizioni meteo e al livello di produzione dell'impianto fotovoltaico. La centralina invierà una serie di dati del veicolo alla casa produttrice per la verifica dei suoi parametri e una pianificazione della manutenzione in base alle reali condizioni dello stesso.

Esempio 3 → Assistenza alle persone

Le nuove tecnologie connesse possono diventare un importante ausilio per l'assistenza alle fasce più deboli della popolazione, come ad esempio, gli anziani. Secondo i dati ISTAT del 2019, gli ultrasessantacinquenni sono passati negli ultimi dieci anni da 12,1 milioni a 13,9 milioni, il 23% del totale della popolazione³⁵. Grazie alla connettività e agli Smart Home Speakers sarà possibile mantenere un contatto costante per fornire assistenza quando l'utente lo necessita e sulla base dei propri bisogni e peculiarità (quando lasciamo il genitore

³⁵ https://www.istat.it/it/files/2020/02/Indicatori-demografici_2019.pdf

anziano a casa da solo durante la giornata oppure nell'occasione di una vacanza, etc.). I parametri della salute personale potranno essere monitorati in tempo reale e le condizioni di allarme (avvisi in caso di cadute, parametri fuori norma, allarmi gas e fumo) potranno essere segnalati per garantire interventi in tempo utile al fine di ridurre i rischi di conseguenze negative.

I dispositivi collegati potranno essere programmati e controllati da remoto, aiutando persone che possono avere difficoltà nell'uso diretto.

Esempio 4 → Telemanutenzione e manutenzione predittiva degli ascensori

Nel cambiamento epocale a cui stiamo assistendo, le tecnologie digitali stanno rapidamente sostituendo quelle analogiche, grazie alla connessione tra sistemi fisici e digitali, alla gestione e alla condivisione delle informazioni e alla possibilità di analisi complesse.

In tale ottica, anche il processo di “manutenzione” è stato ripensato per poter anticipare le esigenze di riparazione degli impianti elevatori, prevenendo il fermo impianto e programmando l'attività nei momenti meno disagiati per il cliente.

Se si considera infatti che gli ascensori sono fondamentali per consentire a chiunque di spostarsi velocemente, confortevolmente e in sicurezza all'interno degli edifici, è facile intuire l'importanza di assicurare il mantenimento continuo della funzionalità degli impianti. A tal fine, sono quindi state studiate diverse soluzioni per cercare di raggiungere tale obiettivo.

Tra queste, la “manutenzione predittiva” sfrutta l'IoT e i big data per ridurre al minimo sia il numero di “fermo impianti” sia il tempo di intervento, garantendo così la massima efficienza e affidabilità di un impianto: attraverso il monitoraggio continuo da remoto di un set di parametri funzionali è infatti possibile capire, in tempo reale, se sia necessario intervenire raccogliendo, al contempo, informazioni utili per creare nuovi modelli di servizio. Una delle altre possibili soluzioni, consiste nell'effettuare la manutenzione tramite la “realtà aumentata”, tecnologia abilitante che permette di visualizzare direttamente in loco, tramite occhiali, tablet, smartphone, ecc., tutte le informazioni che servono al manutentore per poter operare correttamente sull'impianto. Attraverso tale strumento è anche possibile contattare la centrale operativa per richiedere supporto immediato.

Uffici: esempio di Servizio, vantaggi e fruibilità

Andando ad analizzare la struttura dei costi di una attività fisicamente collocata all'interno di un edificio ad uso ufficio si verifica che, generalmente, la voce di costo più significativa è quella relativa ai costi del personale che prestano il loro servizio per l'attività stessa.

Fra le altre principali voci di costo compaiono, nella maggioranza dei casi, il costo per l'affitto della struttura e i costi di conduzione della struttura stessa (costi dell'energia termica ed elettrica, costi di manutenzione).

In questo contesto, rivestono grande importanza tutte le Applicazioni che possono consentire di migliorare l'efficienza dell'attività. Tali miglioramenti possono essere ottenuti lavorando su diversi aspetti:

- Aumento della produttività del personale. È dimostrato che operare in ambienti confortevoli, dove le caratteristiche ambientali e climatiche sono vicine alle proprie esigenze, migliora la produttività e riduce i periodi di assenza dal lavoro. Le tecnologie IoT possono abilitare specifici Servizi per andare in questa direzione.
- Riduzione dei consumi energetici e riduzione dei costi di manutenzione possono essere ottenuti grazie ai Servizi “orizzontali”, già descritti nel paragrafo precedente, che trovano una implementazione piuttosto efficace proprio negli edifici ad uso uffici.

Uno dei problemi che ostacola lo sviluppo di queste Applicazioni è spesso la difficoltà di contemperare le esigenze e gli impegni della proprietà dell’edificio, soggetto che dovrebbe sostenere i costi degli interventi, con quelle dei conduttori che poi godono dei vantaggi derivanti dagli interventi stessi. Andrebbero studiate forme di incentivazione e/o anche nuove tipologie di contratti di locazione, che consentano di superare questa dicotomia di interessi.

Esempio 5 → Work Place Efficiency

Da tempo è stato verificato che il livello di efficienza del personale che opera all’interno di un ufficio è correlato anche al benessere fisico che il posto di lavoro garantisce ad ogni singolo addetto. E allo stesso tempo è altrettanto noto che le condizioni che contribuiscono a migliorare tale benessere sono diverse da persona a persona.

Allo stesso tempo il posto di lavoro fisico ha subito grandi cambiamenti. Oggi si opera sempre più spesso in ambienti “open space”, a supporto dei quali è possibile realizzare degli impianti sempre più sofisticati che sono in grado di monitorare e garantire specifiche condizioni (di luce, di temperatura, di umidità, ecc.) nelle diverse zone e per le diverse attività.

Oggi è anche possibile, all’interno di un ambiente, raccogliere e tracciare gli spostamenti di una persona grazie a tecnologie di geo-referenziazione basate sui telefoni cellulari o su tag di riconoscimento della persona stessa, spesso usati per Servizi quali la rilevazione delle presenze o il controllo degli accessi.

Dall’unione di queste informazioni (condizioni ambientali, posizione della persona, ecc.), tramite opportuni moduli software denominati analytics, è possibile ricostruire le preferenze/abitudini delle persone e, con apposite App, aiutarle a trovare la postazione che meglio si avvicina, anche in momenti specifici della giornata, alle condizioni desiderate.

Una ulteriore evoluzione di questi Servizi (in questo senso si veda anche il prossimo esempio relativo al Servizio basato sullo Human Centric Lighting) può consentire di creare delle vere o proprie zone climatiche all’interno di un open-space, sulla base di esigenze di gruppi di persone, per ottimizzare l’uso dell’energia e contribuire alla riduzione dei consumi, seppure garantendo un altissimo comfort lavorativo.

Ovviamente questi Servizi vengono realizzati secondo quanto previsto dalle vigenti normative, nel massimo anonimato e nel rispetto della privacy.

Esempio 6 → Human Centric Lighting

Lo Human Centric Lighting (HCL) è un concetto sviluppato dalle industrie dell'illuminazione, inteso a promuovere il benessere, l'umore e la salute delle persone, garantendo un adeguato comfort visivo. Può migliorare la concentrazione, la sicurezza e l'efficienza sul posto di lavoro o in ambienti formativi/scolastici. L'illuminazione influenza, positivamente e/o negativamente, la salute umana. Migliorare la qualità della luce ha un effetto noto sia per la visione che per la salute, e a tal fine esistono vari possibili Servizi per i diversi contesti che caratterizzano la nostra vita quotidiana. Oggi, specifiche soluzioni di illuminazione possono essere prodotte e installate in modo da supportare il ritmo circadiano umano, migliorare i livelli di concentrazione ed il benessere generale.

Queste soluzioni si basano su sistemi elettronici di gestione della luce, modulando l'illuminazione artificiale all'interno di edifici e sincronizzandola con il ritmo circadiano dell'uomo o con parametri vitali rilevati da sensori biometrici. La distribuzione della luce è regolata in base alle diverse condizioni della luce diurna e alle specifiche esigenze degli individui durante il giorno. In questo modo, i cambiamenti dinamici della temperatura di colore e dell'illuminamento, in aggiunta ad un'ampia distribuzione della luce da fonti dirette e indirette, stimolano l'organismo umano.

È possibile oggi realizzare sistemi che integrano soluzioni di Building Automation ed i dati ambientali che questi sistemi mettono a disposizione (luminosità, temperatura, qualità dell'aria, umidità) ed implementare algoritmi specifici che permettono di mettere in relazione questi dati con parametri vitali dell'individuo, eventualmente acquisiti attraverso sensori biometrici. La combinazione e la relazione tra questi parametri e la tipologia di ambiente permettono di determinare come output le condizioni di illuminamento (ed eventualmente di colore della luce) ideali per il benessere degli individui.

Negli uffici, l'aumento della motivazione, dell'umore e dell'energia dei dipendenti sono solo due dei molti vantaggi portati dall'utilizzo di soluzioni HCL. Per esempio, dopo pranzo le lacune tipiche di produttività possono essere alleviate da regolazioni dinamiche di direzionalità, illuminamento e temperatura colore della luce, supportato da luce calda diretta e luce indiretta.

Anche in questo caso le soluzioni IoT e l'integrazione con il Cloud rappresentano un fattore abilitante che permette la realizzazione e velocizza lo sviluppo di questa specifica tipologia di Servizi.

Esempio 7 → Controllo e gestione di accessi e spostamenti all'interno di edifici non residenziali

La progettazione "a dimensione di passeggero" è il primo passo per dotare gli edifici di ascensori "intelligenti", in grado di adattarsi alle specifiche esigenze di trasporto degli utenti. Per esempio: negli edifici residenziali, solitamente caratterizzati da altezze non elevate, si devono gestire flussi di traffico modesti, mentre negli uffici si devono ottimizzare picchi di traffico intensi e concentrati nelle fasce orarie di entrata ed uscita dei dipendenti, oltre a notevoli spostamenti di persone all'interno dell'edificio. In quest'ultimo caso, è quindi

necessario garantire la massima flessibilità di esercizio, allo scopo di ottimizzare la gestione del traffico passeggeri, evitando "code" e rallentamenti negli spostamenti interni tra i piani. A tal fine, sono quindi state pensate e sviluppate apposite soluzioni – basate sul principio del "controllo della destinazione" – che "riconoscono" la destinazione di un passeggero prima che esso sia entrato nella cabina dell'ascensore.

In tal modo, il sistema assegnerà al passeggero, in maniera ottimale, la cabina più vicina o quella che raggiungerà più velocemente il piano richiesto, evitando o riducendo le fermate intermedie e diminuendo il tempo richiesto per raggiungere il piano desiderato. Questi sistemi inoltre sono in grado di "dialogare" con gli altri impianti/dispositivi dell'edificio stesso quali, per esempio, sistemi di controllo accessi e BMS.

Centri Commerciali: esempio di Servizio, vantaggi e fruibilità

Da sempre il mondo Retail si pone come primario obiettivo quello di fornire al cliente una piacevole esperienza di acquisto. All'interno di questo concetto si collocano un'infinità di concetti fra i quali, ad esempio, la riduzione dei tempi di attesa e il comfort personale, che vengono trattati nel seguito come esempi di Servizi.

Naturalmente, a fianco del miglioramento della cosiddetta Customer Experience, si collocano altri obiettivi ed altri esempi di Servizi comuni a tipologie di edifici/mercati già analizzati in precedenza. Il tema del miglioramento dell'efficienza nel consumo dell'energia e del contenimento dei consumi è particolarmente significativo in questi contesti e può avere un impatto importante sul conto economico delle imprese, soprattutto venendo da un periodo che ha inciso in modo significativo sui risultati economici del settore. Estremamente rilevante questo aspetto nel settore Food, dove la refrigerazione alimentare, per i suoi consumi energetici e per la sua delicatezza dal punto di vista della sicurezza del prodotto, rappresenta un Servizio critico. Sempre su questo tema, sono molto interessanti gli aspetti legati all'integrazione di informazioni nell'ambito di reti di vendita composte da numerosi (anche migliaia) punti di vendita diffusi sul territorio.

Da non trascurare, infine, anche l'utilizzo dei dati provenienti da apparecchiature personali quali gli Smartphone, che possono consentire di raccogliere informazioni dettagliate circa i percorsi di acquisto, le zone di permanenza, i tempi di attesa degli utenti, sia all'interno che all'esterno dei punti di vendita. Tali informazioni possono contribuire in modo significativo al miglioramento dell'esperienza d'acquisto, ma anche risultare significativi per una migliore gestione degli impianti a servizio del punto di vendita.

Esempio 8 → Riduzione dei tempi di attesa alle casse

Fra i dati che vengono raccolti da un moderno centro commerciale sono spesso presenti le immagini dei sistemi di videosorveglianza utilizzate ai fini di sicurezza (durante il giorno per il controllo dei tentativi di furto, durante la notte per la rilevazione di intrusioni).

Le stesse immagini possono essere processate, tramite opportuni software denominati *video analytics*, per determinare il tempo medio in cui i stazionano o comunque rimangono all'interno di

una certa area (l'area delle casse, piuttosto che la coda per uno dei servizi offerti all'interno del centro).

Tali informazioni possono essere utilizzate in tempo reale per un rafforzamento del personale dedicato al servizio (apertura di nuove casse o aumento del personale dedicato al servizio), mentre in un ambito temporale più esteso possono contribuire ad una migliore organizzazione dei turni di lavoro o, addirittura, degli orari di apertura del centro.

Esempio 9 → L'importanza del colore della luce

Come già descritto per i Servizi del settore Uffici, la luce ha una importanza fondamentale non solo nel determinare il livello di comfort, ma anche i comportamenti delle persone.

Ad esempio, molti studi evidenziano che, nel caso di condizioni climatiche con temperature fredde le persone sono attratte dagli ambienti in cui il colore della luce è più caldo (basse frequenze nello spettro della luce visibile); viceversa, in caso di condizioni climatiche con temperature calde, l'attrazione è verso ambienti con colore della luce più freddo (alte frequenze nello spettro della luce visibile).

Sulla base di ciò si possono realizzare Servizi che, grazie ai dati raccolti dalle centraline meteorologiche esterne (condizioni climatiche) e ai dati raccolti dalle telecamere sui flussi delle persone, possono pilotare i sistemi di illuminazione di singoli spazi (negozi) o dell'intero centro commerciale in modo da creare degli ambienti più attrattivi in base ai criteri sopra riportati.

Gli stessi Servizi possono essere basati su piattaforme in grado di apprendere dall'esperienza, valutando gli effetti ottenuti in base alle regole impostate e correggendo le stesse per migliorarne l'efficacia.

Ospitalità: esempio di Servizio, vantaggi e fruibilità

Con riferimento alle attrezzature professionali per food service e ospitalità, la componentistica gioca un ruolo da protagonista con la fornitura di dispositivi e sistemi di sensoristica intelligente che, nei prossimi anni, cambieranno lo scenario della produzione delle apparecchiature professionali e del loro utilizzo.

La connettività offre, a chi produce e a chi acquista le apparecchiature, l'opportunità di contenere i costi grazie ad un controllo da remoto disponibile 24 ore al giorno, 7 giorni su 7, 365 giorni l'anno e di ridurre i tempi di fermo macchina grazie all'analisi dei dati trasmessi in tempo reale, garantendo così un corretto mantenimento delle performance di sicurezza per l'intero ciclo di vita dell'apparecchio. L'analisi dell'enorme quantità di dati raccolti permetterà ai produttori di macchine, in primis, di aumentare la qualità complessiva del prodotto e del servizio, conoscendo con certezza e in tempo reale lo stato d'uso e gli interventi effettuati su milioni di apparecchi installati in tutto il mondo.

Parallelamente l'utilizzo dei dati consentirà di migliorare l'esperienza d'uso dell'utente e abiliterà la possibilità di offrire ulteriori servizi sul fronte ospitalità:

- ⇒ **Sempre più personalizzati.** Questo tipo di servizi contraddistingue in misura maggiore le strutture di alto livello (4-5 stelle), che puntano a fornire servizi esclusivi, a volte penalizzando aspetti quali efficienza operativa/energetica a favore dell'immagine e dello status che si vuole rappresentare nei confronti del cliente.
- ⇒ **Sempre più efficienti ed automatizzati.** Questo trend contraddistingue in misura maggiore le strutture di medio livello (2-3 stelle) che arrivano oggi ad offrire il servizio in modo totalmente automatico, in assenza di personale di servizio per il cliente. In queste strutture tutto, dalla prenotazione via web fino all'arrivo nella struttura e all'ingresso in camera, dalla colazione fino al check-out, è gestito direttamente dal cliente ed in modo automatico. Il controllo dell'edificio è totalmente remotizzato e il solo servizio di pulizia e riassetto è gestito localmente, ma senza contatto con il cliente.

Tra questi due approcci, fra cui sembra esistere un abisso in termini di funzionalità, esiste invece una fortissima somiglianza: la dipendenza di entrambi, per raggiungere obiettivi di efficacia e performance, dalla gestione integrata di tutti i dati relativi all'utente e all'edificio all'interno del quale soggiorna.

Esempio 10 → Apertura porte

L'evoluzione delle serrature motorizzate utilizzate per controllare l'accesso alle camere nelle strutture ricettive rende oggi disponibile con protocolli Bluetooth o NFC (Near Field Communication) il controllo delle serrature stesse.

Grazie a questa possibilità, l'utente può essere riconosciuto dalla serratura motorizzata attraverso il suo Smartphone e, ove autorizzato, la stessa procede a sbloccare l'accesso. Eventuali Servizi per Smartphone messi a disposizione dalla struttura consentono all'utente stesso di estendere la possibilità di accesso ai familiari, di programmare la propria presenza e i parametri di comfort della stanza.

Da remoto, il responsabile della struttura può gestire le prenotazioni e gli accessi, oltre che avere una visibilità completa sulla presenza degli ospiti. Il Servizio può essere esteso anche alle serrature esterne di accesso alla struttura (cancelli pedonali e carrai, accesso principale), eventualmente aumentando il livello di sicurezza tramite una tastiera di digitazione, che prevede l'inserimento di un PIN che può essere inviato all'ospite (una volta identificato) in tempo reale, tramite ad esempio SMS.

Esempio 11 → Personalizzazione dell'esperienza utente

I moderni alberghi, anche di categoria non elevata, dispongono in genere di sistemi che sono in grado di regolare i principali impianti di camera. Fra questi possiamo citare il sistema di climatizzazione (riscaldamento, raffrescamento), il sistema di illuminazione (accensione, spegnimento, intensità luminosa), fino ad arrivare ai serramenti motorizzati e i sistemi di

intrattenimento multimediale. Queste regolazioni vengono utilizzate dall'utente per adattare la camera alle proprie esigenze e al livello di comfort personale.

Le regolazioni impostate, in presenza di un sistema BMS (Building Management System), sono disponibili e vengono generalmente riconfigurate giornalmente o quando l'utente abbandona la camera.

La semplice associazione di tali informazioni all'anagrafica dell'utente, generalmente facente parte del sistema di prenotazione, può consentire di ricreare le stesse condizioni quando la persona tornerà a far visita alla struttura. Nel caso delle catene di alberghi, che generalmente dispongono di una anagrafica centralizzata, lo stesso servizio potrà essere offerto presso tutti gli alberghi della catena.

[I dati, l'Edificio 4.0 e le normative di riferimento](#)

Lo scenario tecnologico fin qui delineato conferma che la progressiva digitalizzazione, che sta pervadendo da alcuni anni il manifatturiero, sarà la chiave di volta per determinare un reale processo di ammodernamento dei nostri edifici. E come evidenziato nei capitoli precedenti, la crescente richiesta di integrazione, la capacità di acquisire dati, di processare e gestire le informazioni, di creare Applicazioni a partire dai dati generati dai Servizi stessi, costituirà la base sulla quale creare valore, strutturando nuovi servizi, delineando nuove possibilità di mercato. La prospettiva dell'Edificio 4.0 è oggi un obiettivo raggiungibile, grazie alla disponibilità di tecnologie e competenze accessibili, una opportunità quindi di trasformazione e crescita anche per l'intera filiera delle costruzioni, fermo restando un chiaro "indirizzo" in tal senso, sia legislativo sia di normativa tecnica, e la condivisione di una strategia di rinnovo ed ammodernamento del nostro patrimonio immobiliare da parte di tutti gli attori coinvolti.

Attualmente il quadro di riferimento normativo nazionale a sostegno della digitalizzazione degli edifici è del tutto inadeguato. Si registra qualche segnale incoraggiante, per lo più riferito a specifici Servizi (es. obbligo di installazione di sistemi BACS almeno in Classe B (rif. UNI EN 15232) negli edifici terziari nuovi o soggetti a ristrutturazione, obbligo disatteso nella maggioranza dei casi; sostituzione misuratori fiscali con apparecchiature smart, per abilitare servizi di demand-response; ecc.), ma nella oggettiva mancanza di una prospettiva d'insieme sull'evoluzione degli edifici nazionali si annida quella incapacità di passare dalle intenzioni ai fatti. Eppure abbiamo a disposizione un modello di riferimento e di successo, ossia il piano Industria 4.0, che ha dimostrato come la strada della digitalizzazione sia una opportunità di rinascita per l'industria, una occasione per cogliere il treno della innovazione e accrescere la propria competitività, un processo coerente con uno sviluppo industriale sostenibile e circolare.

In ambito europeo la nuova direttiva UE sulla prestazione energetica nell'edilizia, la direttiva 844/2018, nota come EPBD III, si contraddistingue proprio per l'attenzione che riserva all'utilizzo di tecnologie "intelligenti" ed in particolare ai sistemi di automazione e controllo (BACS) negli edifici. Trattasi di un primo ma importante segnale, soprattutto in quanto formalmente si collegano gli obiettivi di efficientamento energetico delle costruzioni con le prospettive di una evoluzione digitale del patrimonio immobiliare. Purtroppo nella EPBD III le buone intenzioni non si traducono del tutto in prescrizioni vincolanti per gli Stati, ma è solo una questione di tempo, visto che la Commissione

europea, con la pubblicazione del Green New Deal a dicembre 2019 e delle prime indicazioni operative ad esso collegate, ha già evidenziato la prossima pubblicazione della nuova Strategia “Built Environment”, strutturata su cinque pilastri: economia circolare, efficienza energetica e dei materiali, clima, **digitalizzazione**, procurement.

Tornando alla EPBD III, rispetto alla precedente normativa EPBD, si introduce il concetto di SRI - Smart Readness Indicator - quale indicatore del livello di “intelligenza” dell’edificio. Come poc’anzi evidenziato, l’attenzione del legislatore comunitario si focalizza non solo sui Servizi/Applicazioni che attengono alla performance energetica, ma l’ambito di valutazione viene esteso a tutti i Servizi/Applicazioni di edificio.

L’ SRI è il risultato di una formula matematica (ancora in discussione al momento della pubblicazione di questo libro) in cui vengono considerati vari Servizi/Applicazioni. E’ interessante rilevare che alcuni di questi sono i medesimi già presenti nella norma tecnica UNI EN15232, standard facente parte della famiglia di norme che sottendono alla EPBD. La UNI EN 15232 ha infatti lo scopo di classificare i Servizi presenti all’interno di un edificio e di valutare il loro impatto sulla performance energetica dello stesso. In particolare considera i seguenti Servizi:

1. riscaldamento
2. acqua calda sanitaria
3. raffrescamento
4. ventilazione controllo umidità e aria condizionata
5. illuminazione
6. schermature solari
7. gestione tecnica
8. rilevamento guasti
9. rapporti sui consumi
10. gestione del set point ambiente
11. gestione FER (Fonti Energia Rinnovabili o RES, Renewable Energy Sources)
12. cogenerazione (CHP, Combined Heat and Power production)
13. smart Grid

L’SRI, partendo dalla medesima logica orientata all’analisi dei Servizi/Applicazioni negli edifici, non poteva che condividere l’approccio metodologico già sperimentato con la UNI EN 15232, focalizzando la metodologia di calcolo in elaborazione sui Servizi prima elencati, ma considerandone anche altri, tra cui:

- generazione di energia in situ
- gestione della domanda-offerta energetica e interazione con la rete (Smart Grid)
- ricarica dei veicoli elettrici e gestione carichi di edificio
- monitoraggio e controllo dei consumi
- altri Servizi non direttamente connessi alla gestione energetica (es. monitoraggio stato di salute degli occupanti, rilevamento e allarme inattività, notifica segnalazioni di emergenza, ecc.)

INDICATORE

DOMINI

SERVIZI

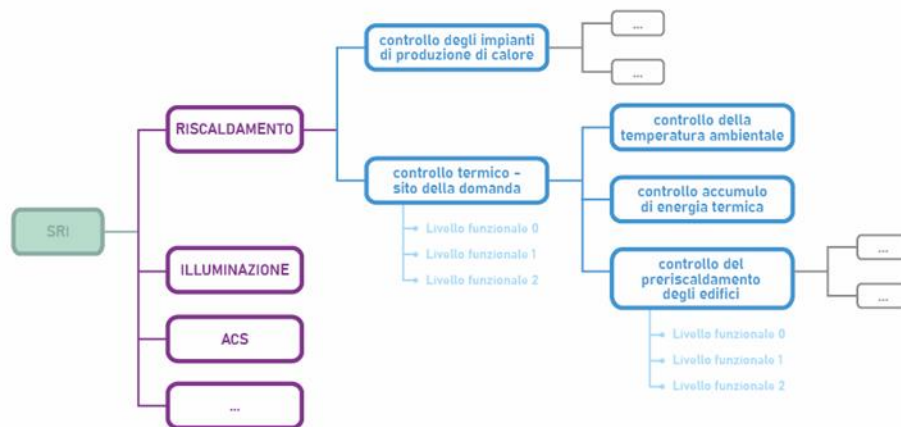


Figura 26: La struttura dell'SRI

Parallelamente all'SRI, la Smart Building Alliance (SBA) for Smart Cities, fondata in Francia nel 2012, sta contribuendo allo sviluppo di R2S (Ready to Services), un framework che in parte complementa ed in parte rivisita in maniera più orizzontale la visione per domini proposta dallo SRI.

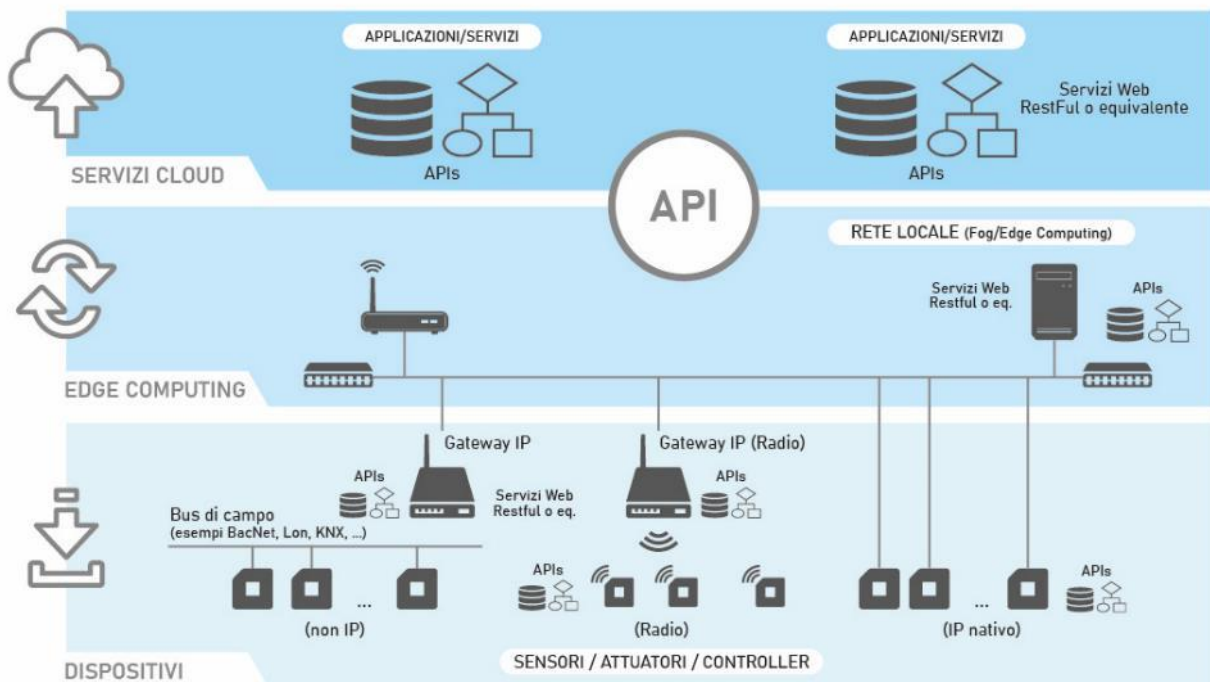


Figura 27: La struttura del R2S

Il concetto R2S propone un unico approccio e si applica a tutti i tipi di building, da nuove costruzioni a ristrutturazioni nel mondo residenziale, alloggi collettivi, terziario, industria, ecc. La sua architettura è caratterizzata da tre livelli:

1. Equipements Terrain (Equipment)

È il campo di un edificio R2S ed è su questo livello che intervengono sensori e attuatori. Queste apparecchiature consentono il controllo dell'edificio, da remoto o automaticamente, sia per l'illuminazione, riscaldamento, tapparelle, ecc. Questo strato di sensori raccoglie dati e comunica attraverso i protocolli di campo con lo strato IP dell'edificio.

2. Reseau du Batiment (Edge Computing)

È questo livello di rete che consente, grazie a gateways ed Edge computers, di ottenere/pre-elaborare le informazioni che saranno tradotte in servizi. Sempre su questo strato si posizionano i multi-service gateways, quei dispositivi in grado di offrire servizi a livello locale controllabili ed aggiornabili centralmente dallo strato sovrastante.

3. Cloud Services

È l'ultimo strato di R2S, il “cervello” dell'edificio, che consente di ospitare e far circolare i dati su diverse piattaforme, controllare ed aggiornare le applicazioni residenti negli strati inferiori (modelli ed algoritmi pre-addestrati a livello Cloud ed “incorporati” a livello Edge), garantire l'integrità e la sicurezza della comunicazione con gli strati inferiori nel tempo (attraverso aggiornamenti remoti di FW, SW e patch di sicurezza). È tipicamente caratterizzato da un HUB che si occupa di device, data e application management, facendo in modo che i dati possano essere proposti e consumati ad un livello superiore. Grazie al Cloud, i dati vengono duplicati, trasformati e rielaborati per consentire l'accesso ad altre applicazioni e sistemi informativi che li trasformano in servizi, siano essi rivolti agli amministratori, agli utenti dell'edificio o qualsivoglia altro stakeholder.

Questa architettura standardizzata offre una possibile risposta al problema dell'interoperabilità, consente maggiore flessibilità e non impone un'infrastruttura dedicata. L'indipendenza tra questi tre livelli è essenziale e fa parte del prerequisito per determinare se e quanto un edificio è Ready2Services. Tale framework ripropone e presenta una rivisitazione in ambito building del paradigma multi-strato che caratterizza le più moderne architetture IoT.

Cybersecurity e privacy in un mondo digitale

Nell'affrontare il tema della sicurezza e della privacy dei dati trattati nell'ambito delle tecnologie digitali è doveroso premettere la distinzione tra dati personali e dati non personali.

*Infatti, i dati personali, intesi come qualsiasi informazione riguardante una **persona fisica** identificata o identificabile, hanno una particolare tutela di legge; i dati diversi da quelli personali, invece, in generale non hanno ad oggi una regolamentazione loro specificamente dedicata.*

È però evidente che, anche con riguardo ad alcune tipologie di dati appartenenti alla seconda categoria, possono esserci esigenze di sicurezza che, proprio in vista di una digitalizzazione spinta dei settori, building compreso, possono manifestarsi in modo molto netto, come attesta il dibattito in corso sulla cyber security. Considerata l'elevata rilevanza economica che tali dati possono avere, gli operatori non potranno fare a meno di tenere in debito conto gli aspetti di sicurezza digitale.

Sicurezza nell'IoT

Sicurezza del dato, privacy, risk management

Il tema della sicurezza del dato è pervasivo nella società informatizzata ed è forse uno degli aspetti più complessi, dal momento che intervengono elementi tecnici e di natura normativa.

È pertanto necessario identificare le aree principali di intervento, ovvero l'identità del dispositivo, l'integrità del software, la robustezza del canale di comunicazione e la confidenzialità del dato.

L'identità del dispositivo riguarda appunto la certezza che il dispositivo con cui si sta interagendo sia proprio materialmente quello. In altre parole, è necessario che all'immagine immateriale del dispositivo, ottenuta tramite il flusso dati da esso proveniente, corrisponda il dispositivo materiale che ci aspettiamo. Per esempio, per un IoT Gateway installato in un edificio, tutelare l'identità del dispositivo significa in primo luogo avere la certezza che il dispositivo non sia stato sostituito (fisicamente o logicamente) con uno dal comportamento analogo, ma in grado di effettuare ulteriori operazioni indesiderate (furto dell'identità).

Oltre alla tutela dell'identità del dispositivo bisogna poi accertarsi dell'integrità, sia fisica del dispositivo (tampering) che quella informatica (hacking). Con tutela della integrità fisica si intende la messa a punto di tecniche che permettono di accorgersi se il dispositivo viene aperto o se gli vengono "aggiunti" altri componenti estranei quali ad esempio memorie. Le strategie anti manomissione fisica prevedono l'uso di particolari componenti che entrano in azione qualora il dispositivo IoT venga sottoposto a manipolazione: esempi sono interruttori e sensori che rilevano l'apertura o il sollevamento del dispositivo. Anche le tecniche costruttive dei dispositivi stessi si stanno evolvendo dall'anti-vandalismo (azioni meccaniche) verso la protezione da attacchi di tipo elettromagnetico e simili.

Con integrità informatica o logica si intende che non siano stati modificati o sostituiti i programmi originariamente installati.

La certezza dell'integrità del dispositivo richiede meccanismi di protezione di natura crittografica che sono strettamente legati al software installato sul dispositivo.

Anche in questo caso i produttori di sistemi IoT sono in grado di offrire delle protezioni; la situazione è tuttavia molto varia ed il livello di copertura cambia anche di molto da costruttore a costruttore.

I più avanzati meccanismi di protezione di natura crittografica creano un rapporto simbiotico tra l'hardware ed il software; un esempio di tale cooperazione è data dai moduli TPM ("Trusted Platform Module"), dei chip altamente specializzati che consentono di effettuare operazioni crittografiche e di memorizzare in aree sicure dati come le chiavi crittografiche ed i certificati di origine.

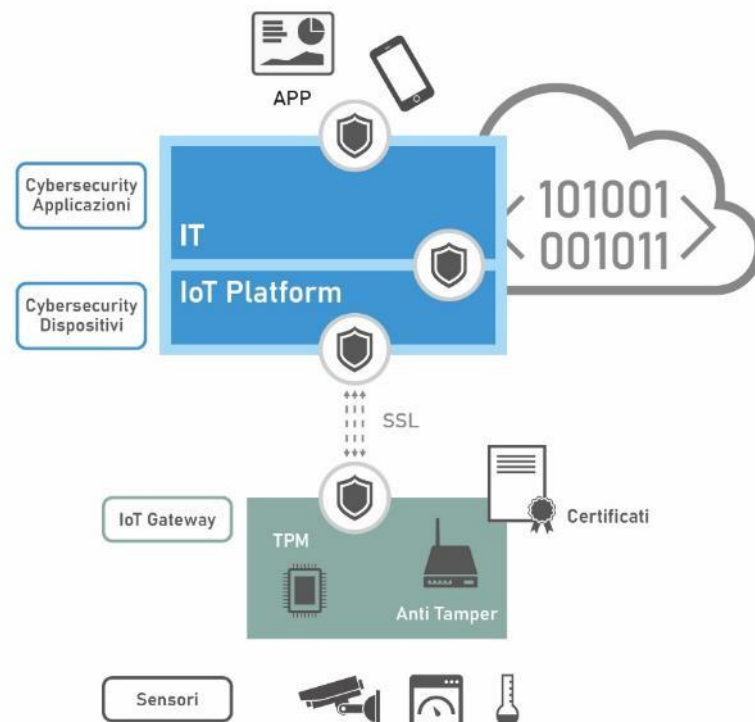


Figura 28: La sicurezza in ambito IoT

La protezione informatica dei dispositivi comincia dal momento della accensione del dispositivo; in questo caso, una valida soluzione è il Secure Boot, che consente di mantenere una catena di autenticazione ("Chain of Trust") dall'accensione fino al trasferimento del controllo al Sistema Operativo. Una concatenazione sicura dell'esecuzione dei programmi evita che si infiltrino e vadano in esecuzione programmi indesiderati, come spyware, malware o virus informatici.

Salendo di livello, il sistema operativo e le applicazioni utente possono essere sottoposte ad autenticazione mediante l'impiego di certificati e chiavi crittografiche; in caso di non corrispondenza dei codici, il software non verrà mandato in esecuzione.

La terza area di intervento è data dalla confidenzialità e sicurezza delle informazioni scambiate tra il dispositivo di campo (sia esso un sensore che un Gateway IoT) ed è data dalla robustezza del canale di comunicazione; anche in questo caso esiste un livello fisico ed uno logico.

Gli aspetti relativi agli attacchi fisici al canale di comunicazione sono piuttosto complessi ed includono tanto l'interruzione del servizio (Jamming, DDoS, etc.) quanto l'intercettazione del dato.

Nel primo caso esistono diversi approcci per mitigare gli effetti di un attacco, come ad esempio dotare il dispositivo di un canale secondario di comunicazione.

Il secondo caso, in cui vi siano tentativi di intercettazione logica del dato, è ben caratterizzato, dal momento che le tecniche di hacking sono spesso le stesse utilizzate per qualsiasi dato che sia fruibile su una rete IP. Ritroviamo dunque le stesse strategie di protezione, come quelle basate su SSL ("Secure Sockets Layer"), mutua autenticazione e simili.

L'ultima area di intervento è la sicurezza e confidenzialità del dato una volta ricevuto e messo a disposizione nel Cloud (o Piattaforma di Integrazione). È qui che il dato viene memorizzato e consumato, da un punto di vista tecnico prima ancor che giuridico, ed è qui che l'attenzione viene posta.

Da un punto di vista fisico, il Cloud rappresenta un importante passo avanti rispetto alla sicurezza del dato, dal momento che i fornitori di questo tipo di servizio sono in grado di investire per la sicurezza una quantità di risorse irraggiungibile per qualsiasi azienda non dedicata. In aggiunta a questo tipo di protezione, vale la pena di ricordare che il Cloud semplifica enormemente la replicazione geografica del dato e delle applicazioni, offrendo così una tutela anche nei confronti di eventi catastrofici (naturali e non).

Da un punto di vista logico, sulla superficie di attacco esposta nel Cloud (interfaccia di accesso) ritroviamo delle minacce simili a quelle a cui sono esposti i dispositivi sul campo, e di conseguenza anche le soluzioni sono analoghe: l'impiego di certificati ed altre tecniche crittografiche consente di garantire la protezione del dato dalla sua generazione fino all'inserimento nel Cloud stesso.

Una volta che il dato è stato ingerito nella Piattaforma di Integrazione, si trovano nuove minacce poiché cambiano le possibili strategie di attacco (furto di credenziali, sfruttamento di bug nelle interfacce utente e nelle API di programmazione, vulnerabilità del Sistema Operativo, eccetera). La maggior parte di questi attacchi sono difficilmente gestibili con un approccio tradizionale, a causa della grande specializzazione richiesta per evitare o correggere situazioni di rischio, e per i costi e tempi che tali attività aggiungono alla operatività quotidiana. Al contrario, i principali fornitori di servizi Cloud sono assolutamente dedicati allo studio, prevenzione e risoluzione di questo tipo di problema (un esempio è stata la scoperta di due falle nella sicurezza della maggior parte delle moderne CPU).

Da ultimo, oltre alla sicurezza del dato, esiste l'aspetto relativo alla privacy, ovvero a come il dato stesso viene manipolato ed esposto. A ciò si aggiunge il fatto che le informazioni potrebbero essere generate, raccolte e processate in modo del tutto automatico e trasparente.

Non esiste probabilmente una risposta di natura tecnologica al problema della privacy; la discussione su come affrontare la questione è ancora molto vivace e probabilmente si articolerà ancora di più man mano che l'IoT aumenterà la sua diffusione. È ragionevole ipotizzare che dal dibattito etico, filosofico e politico possa emergere un quadro giuridico che definisca i confini entro i quali sia legittimo operare, esattamente come già accade in altri ambiti altamente sensibili (sanità, difesa, settore bancario, e così via).

Privacy dei dati: raccolta, conservazione e diffusione

Nell'ambito dell'attuale legislazione, la "Privacy" dei dati è riferita ai **dati personali** cui, a garanzia della loro riservatezza, sono riconosciute particolari tutele dal Regolamento (UE) n. 679/2016, il cosiddetto *General Data Protection Regulation* (GDPR) direttamente applicabile in tutti gli Stati membri dal 25 maggio 2018³⁶.

Per "dato personale" si intende qualsiasi informazione riguardante una **persona fisica** identificata o identificabile, laddove si considera identificabile la persona fisica che può essere accertata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale³⁷.

Non si considerano quindi dati personali e sono esclusi dal GDPR i dati riferiti a persone giuridiche, quali i dati riferiti a società (si pensi, ad esempio, ai dati raccolti con le nuove tecnologie dell'Industria 4.0) che troveranno tutela eventualmente tramite altre discipline di legge, quali quella a tutela di *know-how*, brevetti e in generale delle privative industriali.

A tutela della riservatezza dei dati personali come sopra intesi, il GDPR impone una serie di obblighi di cui risponde il cosiddetto **titolare** del trattamento, ossia la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali³⁸.

Nell'individuazione di tali obblighi, una delle novità più rilevanti introdotte dal GDPR è la cosiddetta **privacy (o data protection) by default³⁹ and by design⁴⁰** che comporta la necessità di configurare il trattamento, prevedendo fin dall'inizio le garanzie indispensabili al fine di soddisfare i requisiti del regolamento e tutelare i diritti degli interessati – tenendo conto del contesto complessivo ove il trattamento si colloca e dei rischi per i diritti e le libertà degli interessati.

La novità è che tutto questo deve avvenire a monte, prima di procedere al trattamento del dato vero e proprio e si richiede, pertanto, un'**analisi preventiva del rischio** inerente al trattamento e un

³⁶ Il regolamento 679/2016 è stato pubblicato sulla G.U.U.E. n. L 119 del 4 maggio 2016 e sostituisce la precedente disciplina comunitaria dettata con la direttiva 95/46/CE, recepita in Italia dapprima con la legge 676/1996 e poi con il D. Lgs. 196/2003, il cosiddetto Codice Privacy.

³⁷ Categorie particolari di dati personali, il cui trattamento è vietato salvo in presenza di specifici presupposti, sono i dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, i dati genetici, i dati biometrici intesi a identificare in modo univoco una persona fisica, i dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

³⁸ Oltre al titolare, ricordiamo comunque la figura del responsabile del trattamento, inteso come la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento e quella del *Data Protection Officer* che va nominato in alcuni casi.

³⁹ La **privacy by default** è intesa come obbligo di mettere in atto misure tecniche e organizzative adeguate a garantire che siano trattati, di default, solo i dati personali necessari per ogni specifica finalità del trattamento; ciò vale per la quantità dei dati raccolti, l'estensione del trattamento, il periodo di conservazione e l'accessibilità.

⁴⁰ La **privacy by design** è intesa come obbligo, sin dalla fase di progettazione e sviluppo di un nuovo servizio o prodotto e di una modalità di trattamento, di mettere in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione ed a integrare nel trattamento le necessarie garanzie.

impegno applicativo da parte dei titolari che devono sostanziarsi in una serie di attività specifiche e dimostrabili.

Per quanto riguarda quindi i dati personali “digitali”, fin dalla fase di progettazione dei servizi e dei prodotti, gli operatori coinvolti dovranno valutare la possibilità di adottare soluzioni tecnologiche a garanzia della privacy degli utenti, con trattamento dei soli dati necessari per le finalità che si vogliono raggiungere (...e per le quali gli utenti abbiano dato il loro consenso).

Esempio: la geolocalizzazione negli smartphone. Nel quadro della precedente disciplina, se l'utente non voleva essere geolocalizzato poteva disattivare questa funzione. Con il GDPR invece la funzione si potrà attivare solo su richiesta dell'utente⁴¹.

Il GDPR conferma poi i seguenti aspetti della precedente disciplina che, assieme alla privacy by default e by design, rappresentano per così dire i fondamenti della tutela della privacy:

- ogni trattamento di dati personali deve rispettare alcuni principi base
- gli interessati, ossia le persone cui i dati personali si riferiscono, devono ricevere un'informativa sull'uso dei loro dati e prestare il proprio consenso a tale utilizzo
- agli interessati sono riconosciuti alcuni diritti fondamentali circa i loro dati che gli stessi possono esercitare in qualsiasi momento
- vanno adottate adeguate misure di sicurezza nel trattamento e nella conservazione dei dati personali

Nel dettaglio, i **principi base** che ogni trattamento di dati personali deve rispettare, sono:

- a) liceità, correttezza e trasparenza⁴²
- b) limitazione della finalità: i dati debbono essere raccolti per finalità determinate, esplicite e legittime e successivamente trattati in modo non incompatibile con tali finalità
- c) minimizzazione dei dati: i dati debbono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati
- d) esattezza: i dati debbono essere esatti e, se necessario, aggiornati
- e) limitazione della conservazione: i dati sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati
- f) integrità e riservatezza: i dati devono essere trattati in maniera da garantirne un'adeguata sicurezza, compresa la protezione, mediante misure tecniche e

⁴¹ Si tratta di un esempio applicativo dato dal Garante privacy <Finora, se non volevamo essere geolocalizzati dovevamo disattivare questa funzione. Con le nuove norme europee sulla protezione dei dati, che saranno applicate dal prossimo anno, le società che progettano questi sistemi avranno un obbligo ancora più cogente di attenersi al principio "privacy by default". Allora il criterio sarà inverso: la funzione non si potrà attivare automaticamente, ma solo su nostra richiesta.>

⁴² Il richiamo al principio della trasparenza (per cui le informazioni destinate al pubblico o all'interessato debbono essere facilmente accessibili e di facile comprensione e deve essere utilizzato un linguaggio semplice e chiaro) rappresenta una rilevante novità sul fronte dei principi generali da rispettare nel trattamento dei dati introdotta dal GDPR.

organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali⁴³

Il GDPR richiede che ogni trattamento debba avere un fondamento giuridico che lo giustifichi e tra questi il principale è il **consenso**: il trattamento è lecito e possibile se *<l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità>*⁴⁴.

Questo è un aspetto centrale da tenere in considerazione anche nella raccolta dati tramite tecnologie digitali, che non può quindi prescindere dall'obbligo di **informare l'interessato** sull'ambito di utilizzo dei suoi dati e di **raccoglierne** previamente il relativo **consenso**: in tale contesto, anche la comunicazione a terzi o la diffusione di dati personali "digitali" saranno possibili solo se l'interessato vi abbia acconsentito.

Va poi richiamata l'attenzione sul fatto che il GDPR stringe le maglie sui tempi per i quali i dati vengono conservati, che non debbono eccedere quelli necessari al conseguimento delle finalità per cui i dati sono raccolti: ne consegue che tra le informazioni da dare all'interessato - e questa è una novità - vi deve essere anche quella relativa al periodo di conservazione dei dati personali oppure, se non possibile, ai criteri utilizzati per determinare tale periodo.

L'interessato inoltre deve essere sempre informato dei diritti che gli sono riconosciuti per legge circa i suoi dati personali, tra cui il diritto di accesso ed il diritto di rettifica. Con il GDPR tali diritti sono stati estesi anche al **diritto all'oblio** (diritto di chiedere la cancellazione dei dati) ed al **diritto alla portabilità** dei dati (che consente all'interessato di ottenere i suoi dati in formato strutturato, di uso comune e leggibile a macchina e di trasferirli ad altri⁴⁵).

Il Codice Privacy, in vigore fino al 24 maggio 2018, prevedeva alcune misure minime di sicurezza da adottare nella conservazione dei dati, che, per quanto riguarda i trattamenti di dati personali effettuati con strumenti elettronici, comprendevano l'adozione di un sistema di autenticazione informatica; l'utilizzazione di un sistema di autorizzazione per l'accesso ai dati; la protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici; l'adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi; l'adozione di tecniche di cifratura o di codici identificativi ma limitatamente ai dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari.

Il Codice prevedeva anche l'obbligo di tenuta di un aggiornato documento programmatico sulla sicurezza, che poi è stato abrogato.

⁴³ Art. 5 GDPR

⁴⁴ Art. 6 GDPR

⁴⁵ Il diritto alla portabilità dei dati è un diritto tipicamente digitale perché non riguarda gli archivi cartacei.

Il GDPR invece non prevede più misure minime, ma **misure di sicurezza tali da garantire un livello di sicurezza adeguato al rischio del trattamento**, da implementare dopo un'analisi degli impatti negativi sulle libertà e sui diritti degli interessati, che tenga conto dello stato dell'arte e dei costi di attuazione nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche.

Il GDPR indica⁴⁶ quindi una lista non esaustiva e di per sé non obbligatoria di tali misure quali:

- a) la cifratura dei dati personali⁴⁷ e la pseudonimizzazione⁴⁸
- b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento
- c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico
- d) l'adozione di una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento⁴⁹

Inoltre, il GDPR impone per tutti i titolari e i responsabili di trattamento, eccetto gli organismi con meno di 250 dipendenti (ma solo se non effettuano trattamenti a rischio), l'obbligo di tenere un **registro delle operazioni di trattamento**⁵⁰. Il Garante Privacy ritiene si tratti di uno strumento fondamentale anche allo scopo di disporre di un quadro aggiornato dei trattamenti in essere all'interno di un'azienda o di un soggetto pubblico – indispensabile per ogni valutazione e analisi del rischio. Il registro deve avere forma scritta, anche elettronica, e deve essere esibito su richiesta al Garante.

Segnaliamo per completezza, tra le altre rilevanti novità del GDPR che possono riguardare anche i dati "digitali", le seguenti:

- In caso di **Data Breach**, ossia di violazioni dei dati personali realizzate da soggetti non autorizzati, obbligo del titolare del trattamento di notificare al Garante le violazioni e, in presenza di determinate circostanze, di estendere tale notificazione anche all'interessato.
- Designazione del **Data Protection Officer** nelle ipotesi in cui il trattamento sia svolto da un ente pubblico, oppure l'attività principale del titolare consista in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il **monitoraggio regolare e sistematico**

⁴⁶ Art. 32 GDPR

⁴⁷ Il Codice privacy impone l'adozione di tecniche di cifratura o di codici identificativi ma limitatamente ai dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari.

⁴⁸ La "**pseudonimizzazione**" anche se non obbligatoria, rappresenta una novità del GDPR: essa prevede che i dati personali non <possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile>.

⁴⁹ Il Garante Privacy peraltro ha già richiamato l'attenzione sulla possibilità di utilizzare l'adesione a specifici codici di condotta o a schemi di certificazione per attestare l'adeguatezza delle misure di sicurezza adottate. Inoltre, facendo anche riferimento alle prescrizioni contenute, in particolare, nell'Allegato "B" al Codice privacy, l'Autorità potrà valutare la definizione di linee-guida o buone prassi sulla base dei risultati positivi conseguiti in questi anni.

⁵⁰ I contenuti del registro sono indicati nell'art. 30 GDPR.

degli interessati⁵¹ su larga scala⁵² o consista nel trattamento sempre su larga scala di dati sensibili o giudiziari (la nuova figura non va confusa con quella del Responsabile del trattamento dei dati, poiché mentre il responsabile risponde al titolare per il proprio operato, il *Data Protection Officer* deve essere autonomo e indipendente).

- Incoraggiamento di **meccanismi di certificazione** della protezione dei dati nonché di sigilli e marchi di protezione dei dati allo scopo di dimostrare la conformità al Regolamento dei trattamenti effettuati dai responsabili del trattamento e dagli incaricati del trattamento.
- Introduzione di **pesanti sanzioni amministrative pecuniarie**.

Le sfide e mercati dell'IoT "sicuro"

Sempre più gli sviluppatori si trovano di fronte all'arduo compito di mettere in piedi ed utilizzare al meglio l'IoT "in modo sicuro", in quanto le soluzioni di sicurezza IT tradizionali, valutate ed adottate dagli staff IT delle Aziende, non sempre rispondono in modo sufficientemente adeguato alle esigenze di sicurezza IoT.

Tenendo presente che i requisiti stringenti della sicurezza delle informazioni fanno riferimento al classico acronimo "RID", ovvero Riservatezza, Integrità e Disponibilità, l'IoT presenta sfide di tipo differente dall'IT, da valutare attentamente, tra le quali:

- aumento di preoccupazioni sulla privacy, un tema che a volte è poco chiaro per i tecnici informatici (hardware e software) coinvolti in progetti e sviluppo di applicazioni IoT;
- sicurezza limitata da vincoli (hardware e software) della piattaforma stessa che i tecnici hanno selezionato per lo sviluppo, che rende una sfida i controlli di sicurezza di base;
- la mobilità estesa e distribuzione degli oggetti nello spazio/territorio, che rende complessi il monitoraggio e la gestione degli asset connessi;
- elevati volumi sia di dispositivi connessi che dei dati raccolti e gestiti, che fanno delle operazioni di aggiornamento dei dispositivi e manutenzione di routine una sfida;
- operazioni, attività ed elaborazione di dati ed informazioni basate su Cloud che rendono ogni perimetro di sicurezza meno efficace e poco circoscrivibile.

Nel contempo l'IoT è già una realtà molto presente ed utilizzata nel mondo "consumer", con l'adozione da parte dei consumatori di molti prodotti/servizi già diffusi: oggetti IoT indossabili,

⁵¹ Il considerando 24 GDPR ricomprende nel monitoraggio del comportamento degli interessati tutte le forme di tracciamento e profilazione su Internet anche per finalità di pubblicità comportamentale. Esempi: tracciamento dell'ubicazione, per esempio da parte di App su dispositivi mobili ed inoltre: monitoraggio di dati relativi allo stato di benessere psicofisico, alla forma fisica e alla salute attraverso dispositivi indossabili; utilizzo di telecamere a circuito chiuso; dispositivi connessi quali contatori intelligenti, automobili intelligenti, dispositivi per la domotica, ecc.

⁵² Il considerando 91 GDPR indica come trattamenti su larga scala quelli che mirano al trattamento di una notevole quantità di dati personali a livello regionale, nazionale o sovranazionale e che potrebbero incidere su un vasto numero di interessati e che potenzialmente presentano un rischio elevato

elettrodomestici “Smart”, abitazioni “smart”, negozi “smart”, musei, pubblicità, entertainment, sport, ecc.

Ma IoT è anche sempre più diffuso nel mondo B2B, Industria e nel settore Infrastrutture pubbliche: energia, trasporti, edifici, produzione industriale, grande distribuzione, banche, assicurazioni, pagamenti, salute, difesa, ecc.

Sviluppare sistemi IoT “Sicuri”

Per impostare correttamente progetti di sviluppo IoT che abbiano come base anche concetti di cyber security (intesa come protezione dai rischi informatici delle reti e dei sistemi IoT) suggeriamo di far riferimento alla Guida pubblicata nel 2015 da Cloud Security Alliance (CSA)⁵³. Nella Guida vengono descritte alcune sfide connesse con l'adozione della IoT e una serie di raccomandazioni che possono essere seguite da utilizzatori e sviluppatori di sistemi dell'IoT per soddisfare i seguenti obiettivi:

- mantenere riservatezza e integrità di dati personali e di business raccolti all'interno del sistema IoT attraverso l'utilizzo di crittografia, autenticazione e protezione dell'integrità dell'infrastruttura IoT;
- comprendere ed affrontare i temi della privacy dei soggetti interessati prima dell'implementazione dell'IoT, effettuando una valutazione globale dell'impatto sulla privacy;
- salvaguardare l'infrastruttura dagli attacchi che colpiscono la IoT come vettore e con destinazione gli asset di un'organizzazione, attraverso l'uso di controlli del ciclo di vita del dispositivo IoT e un approccio di security a strati (la cosiddetta layered security/defense in depth);
- avviare un approccio globale per la lotta contro le minacce alla sicurezza attraverso la condivisione di informazioni all'interno della community con fornitori di security, colleghi del settore industriale, i CERT (Computer Emergency Response Team), eventualmente coinvolgendo CSA Cloud Security Alliance.

Cosa valutare per rendere sicuro uno “sviluppo IoT”

Esistono numerosi fattori che possono rendere insicura una progettazione IoT:

- alcuni sistemi IoT sono mal progettati e implementati perché usano protocolli e tecnologie non pensati per IoT e diversi tra loro: questo spesso porta a configurazioni complesse e vulnerabili;
- la mancanza nell'IoT di processi e modelli di business consolidati;
- la mancanza di linee guida di riferimento comuni e riconosciute sia per lo sviluppo che per la manutenzione e per la gestione dei dispositivi IoT;

⁵³ <https://cloudsecurityalliance.org/media/news/csa-launches-new-security-guidance-for-early-adopters-of-the-iot>

- l'IoT in taluni casi introduce problemi di sicurezza fisica, il cui impatto è ancora da valutare correttamente (pensiamo alla possibilità di comandare da remoto impianti potenzialmente pericolosi per l'incolumità delle persone, dell'ambiente e dell'impianto stesso);
- le preoccupazioni sulla privacy sono complesse e non sempre immediatamente risolvibili;
- scarsità di Best Practice disponibili per gli sviluppatori ed utilizzatori di IoT;
- mancanza di Standard e Best Practice condivise per l'autenticazione e l'autorizzazione di dispositivi IoT;
- mancanza di Standard e Best Practice condivise per Incident Management e Response nell'IoT;
- disponibilità limitata di interfacce tra dispositivi IoT, SIEM (Security Information and Event Management), IAM (Identity and Access Management) e applicazioni di Security
- Le norme di security per le configurazioni delle piattaforme virtualizzate IoT e multi-tenancy non sono ancora mature e standardizzate.

Controlli di Security da tenere presenti nell'IoT

Qui evidenziamo alcuni controlli di sicurezza che sono raccomandati per le organizzazioni che intendono sviluppare applicazioni, dotarsi o utilizzare sistemi basati su IoT.

Da notare che sono stati adattati alle specifiche caratteristiche dell'IoT, per consentire alle organizzazioni di mitigare alcuni dei rischi più evidenti associati a queste tecnologie.

1. analizzare l'impatto sulla privacy per i soggetti interessati (tutti gli stakeholder) e quindi adottare un approccio "Privacy-by-Design" nello sviluppo e deployment dell'IoT;
2. applicare approcci "Secure Systems Engineering" e "security-by-design" in fase di disegno, sviluppo e testing dell'IoT;
3. adottare protezioni e security a più livelli per difendere oggetti ed utilizzatori di IoT;
4. implementare Best-Practice condivise per la protezione di dati e informazioni sensibili;
5. definire i controlli per tutto il ciclo di vita dei dispositivi IoT, dal disegno, allo sviluppo, all'utilizzo fino anche alla dismissione per rotture e/o obsolescenza;
6. definire e sviluppare framework di autenticazioni/autorizzazioni per l'ecosistema IoT utilizzando standard condivisi;
7. definire e attuare un quadro di Audit/Logging per l'ecosistema IoT aggiunto ad un sistema di monitoraggio in grado di identificare eventuali anomalie di comportamento e/o utilizzo.

Alcune considerazioni ed aree da guardare con attenzione per la sicurezza IoT

Dopo una prima fase di progetti-pilota e "pionieristica", con tentativi e realizzazioni che hanno indicato la fattibilità e la sostenibilità tecnica di applicazioni IoT, siamo ora al momento delle valutazioni del modello di business e commerciale. Al momento c'è ancora un po' di confusione sia sul ruolo dell'IoT che su modelli di business ed architetture: ad esempio ci sono mercati ed attori in fase di valutazione e raccolta informazioni, ovvero chi parla di IoT "personali/consumer" e chi di "Industrial IoT". Ecco alcune aree e considerazioni che devono essere valutate ai fini di garantire la sicurezza in ambito IoT:

- le differenze tra “Smart Building”, “Smart Home” e “Smart City”, e quelle di tutti gli altri ambiti come: Healthcare, Utility, Manufacturing, Trasporti, veicoli connessi, droni, veicoli a guida autonoma/assistita, dispositivi indossabili, Gaming, vending machines, POS (Point Of Sale), ecc;
- le differenze tra i diversi ecosistemi IoT: protocolli, tipo di dispositivi, processori, architetture, sistemi operativi, tipologia di dati e messaggi, piattaforme, organizzazione e modelli di business;
- i diversi “cicli di vita” delle applicazioni e target di mercato: ad esempio un prodotto consumer e di basso costo può essere destinato ad essere attivo ed utilizzato anche solo per alcune settimane/mesi (un periodo che nei casi estremi coincide con la durata della vita del dispositivo stesso, caratteristica che non lo rende meno “importante” a livello di privacy e di PII Personally Identifiable Information). Al contrario, un device per l’industria, building o utility, può avere un ciclo di vita di anni/lustri: proviamo a pensare ai lampioni di un centro abitato, alle centrali termiche/frigorifere di un edificio, agli ascensori o alle stazioni di pompaggio di un acquedotto. Come bisognerà provvedere agli aggiornamenti di firmware/software o gestire le configurazioni nel tempo? Come “spegneremo” dispositivi obsoleti, “dimenticati” ed abbandonati, che potranno rappresentare future back-door di accesso alle reti di domani?
- che protezione/sicurezza “fisica” possiamo ipotizzare per dispositivi “abbandonati” in cabine di guardiania, in scantinati, in armadi in edifici remoti o shelter sparsi sul territorio, che potrebbero rappresentare porte di ingresso alla rete?
- qual è la linea di demarcazione tra rete IoT, rete dell’utente, rete del manutentore, rete del provider di servizi di connessione e rete dell’organizzazione che la gestisce?
- dove finiscono i sistemi IT dell’azienda e dove inizia la IoT che utilizza e/o fa confluire dati ai quei sistemi IT?
- proviamo a pensare all’impatto che hanno già oggi le politiche aziendali “BYOD” (Bring Your Own Device), ovvero l’utilizzo di dispositivi personali, quali Smartphone e tablet di proprietà dei collaboratori e del personale esterno all’azienda per accedere a dati, informazioni IoT ed applicazioni aziendali;
- valutiamo la Privacy by Design, in quanto applicazioni IoT, che non hanno impatti sulla privacy, messe insieme e connesse ad altre, potrebbero avere impatti sulla privacy: anche utilizzando crittografia ed altri controlli una qualsiasi traccia potrebbe far risalire una specifica transazione ad una specifica organizzazione o persona;
- sappiamo che alcuni protocolli e dispositivi IoT oggi disponibili e largamente utilizzati sul mercato non sono stati pensati fin dall’inizio per essere sicuri, e a volte vincoli di capacità di elaborazione e di banda non permettono l’implementazione di tecniche di autenticazione e crittografia evoluti e necessari agli scopi della Security;
- ancora oggi, nonostante le tante esperienze già realizzate e disponibili sul mercato, ci sono poche persone formate e ridotte best practice sul tema IoT Security e sugli impatti che possono esserci nello sviluppare applicazioni “non sicure”;

- scarseggiano anche esperienze, evidenze e notizie certe riguardo alla gestione di eventuali incidenti dovuti ai problemi di security su reti IoT.

In conclusione, qui ci limitiamo ad una elencazione di alcuni input per fare in modo di avere dei livelli di sviluppo e gestione accettabili già oggi per mettere in piedi IoT più sicure.

Il documento “Security Guidance for Early Adopters on the Internet of Things (IoT)”⁵⁴ è il prodotto del gruppo di lavoro CSA Mobile - IoT Initiative, ed è stato pubblicato ad aprile 2015: il documento è stato creato utilizzando input di un gruppo di esperti di sicurezza e di mobilità provenienti da diversi settori industriali. In questa Guida sono presenti riferimenti e informazioni provenienti da linee guida già esistenti, al fine di evitare duplicazioni e favorire l'allineamento con il lavoro di altri organismi del settore. Inoltre, la guida/documento è stato realizzato in modo tale da consentirne un utilizzo cross-Industry: questo è stato ottenuto esaminando architetture utilizzate in molteplici settori e la selezione di controlli di sicurezza che possano essere tipici di ogni settore.^{55 56}

⁵⁴

https://downloads.Cloudsecurityalliance.org/whitepapers/Security_Guidance_for_Early_Adopters_of_the_Internet_of_Things.pdf

⁵⁵ <http://www.itu.int/itu-t/recommendations/rec.aspx?rec=Y.2060>

⁵⁶ <http://www.iiconsortium.org/wc-security.htm>

Il mercato di riferimento del Building

Non c'è dubbio che l'economia dei dati stia crescendo a ritmi elevati. Più velocemente si riusciranno a digitalizzare le "Cose" e più questa economia crescerà; gli edifici sono tra le "Cose" più importanti da digitalizzare.

Una recente analisi UNCTAD⁵⁷ – United Nations Conference on Trade and Development – pubblicata ad aprile 2020 - traccia il cambiamento del panorama digitale dalla crisi finanziaria 2008/09 ai giorni nostri, in piena crisi finanziaria causata dalla pandemia da Covid19. Il rapporto evidenzia come l'emergenza coronavirus stia accelerando la transizione verso una economia digitale, favorendo la diffusione e l'utilizzo di soluzioni, strumenti e servizi digitali, anche e soprattutto per effetto dei cambiamenti comportamentali richiesti a livello globale per contenere la diffusione del virus. Nel contempo la pandemia, che costringe "confinata" la popolazione a livello globale, sta mettendo in luce tutte le criticità e i limiti di ambienti e contesti "non connessi", rispetto a quelli connessi, paradossalmente indicando nella digitalizzazione non tanto una scelta quanto ormai un percorso obbligato. Il basso livello di digitalizzazione degli edifici, mai come oggi si dimostra e si avverte come una criticità, in un momento storico nel quale è altissima la percezione di alcune Applicazioni, quali la telemedicina, lo smart working, la didattica online e molte altre.

Il mercato delle Costruzioni in Italia pre e post COVID-19

Effetti dell'emergenza sanitaria e andamento del mercato

Nel 2019 la spesa in costruzioni ha registrato tassi di crescita in linea con quelli dell'anno precedente (+2,6%), grazie al buon andamento del mercato immobiliare residenziale, che ha attivato numerosi interventi di riqualificazione (sostenuti dalle agevolazioni fiscali). Le prospettive 2020, all'inizio dell'anno, erano certamente positive, anche in considerazione della conferma dei benefici fiscali e in previsione della definizione del piano di ammodernamento del patrimonio immobiliare, come previsto dalla nuova direttiva comunitaria EPBD. L'impatto del COVID-19 si sta dimostrando devastante anche su questo fronte. Le costruzioni risentono delle misure restrittive legate alla crisi sanitaria, che si applicano anche ai cantieri. Non prima dei mesi estivi, dunque, si prevede potranno ripartire attività e investimenti. Nella media del 2020 Confindustria stima un calo del 9,9% nel settore delle abitazioni e del 7,4% nel settore dei fabbricati non residenziali, mentre nel 2021 è atteso un recupero degli investimenti fissi lordi del 4,4%.⁵⁸

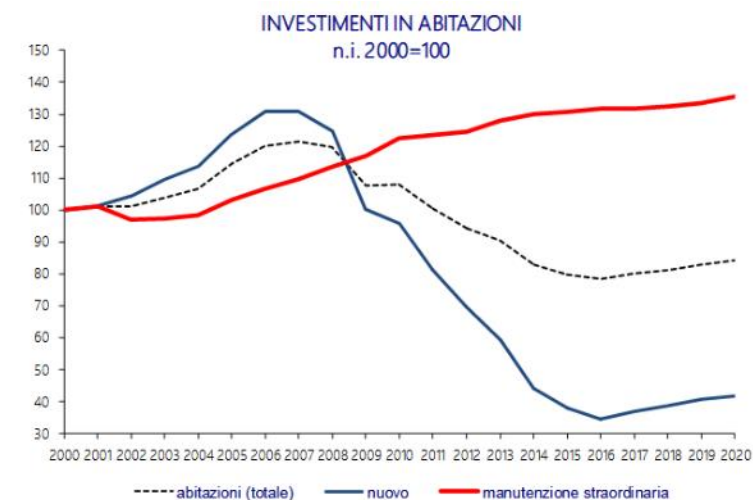
⁵⁷ <https://unric.org/it/covid-19-evidenzia-la-necessita-di-coltmare-il-divario-digitale/>

⁵⁸ CONFINDUSTRIA LE PREVISIONI PER L'ITALIA. QUALI CONDIZIONI PER LA TENUTA ED IL RILANCIO DELL'ECONOMIA? Primavera 2020

Fotografia pre emergenza sanitaria – investimenti 2019

Valutazione delle tendenze del mercato residenziale

Ance, per gli investimenti in nuove abitazioni nel 2019, ha stimato un incremento del 5,4% in termini reali rispetto al 2018, a conferma di una dinamica positiva iniziata nel 2017. Negli anni precedenti, infatti, tale comparto ha subito una drastica contrazione dei livelli produttivi di circa il 70%, risultando il più penalizzato dalla lunga e pesante crisi iniziata nel 2008. L'interruzione del trend negativo per questo comparto è collegato anche all'andamento positivo dei permessi di costruire registrato negli ultimi tre anni. Sulla base dei dati Istat sull'attività edilizia tra il 2016 ed il 2018, si stima che il numero di permessi, Scia e Dia ritirati per la costruzione di nuove abitazioni e ampliamenti sia aumentato del 25%.



Fonte: Ance

Figura 29: Investimenti in abitazioni

Gli investimenti in riqualificazione del patrimonio abitativo hanno confermato la dinamica positiva degli anni precedenti, giungendo a rappresentare circa il 37% del valore degli investimenti in costruzioni. Rispetto al 2018, per gli investimenti in tale comparto si valuta una crescita dello 0,7% in termini reali. Tale stima ha tenuto conto della proroga, fino a tutto il 2020, prevista nell'ultima Legge di Bilancio, del potenziamento al 50% della detrazione per le ristrutturazioni edilizie e della detrazione del 65% per gli interventi di riqualificazione energetica degli edifici. Il risultato del 2019 ingloba anche i primi effetti sui livelli produttivi, seppur contenuti, derivanti dal sisma-bonus ed eco-bonus destinati a interi edifici (condomini).

Le costruzioni non residenziali private: un confronto con il mercato edilizio residenziale

Gli investimenti privati in costruzioni non residenziali hanno segnato un aumento del 2,5% in termini reali nel 2019. La stima ha tenuto conto dei dati particolarmente positivi dei permessi di costruire relativi all'edilizia non residenziale a partire dal 2015. Nei primi tre mesi del 2019 si è registrata una prima battuta di arresto: 7,9%, in termini di nuove superfici concesse, nel confronto con lo stesso periodo dell'anno precedente. Una conferma di questo rallentamento viene anche dai dati sul credito riferiti all'edilizia strumentale: nel corso dei primi nove mesi del 2019 i mutui erogati per investimenti si sono ridotti del 30%, dopo i consistenti aumenti degli anni precedenti.

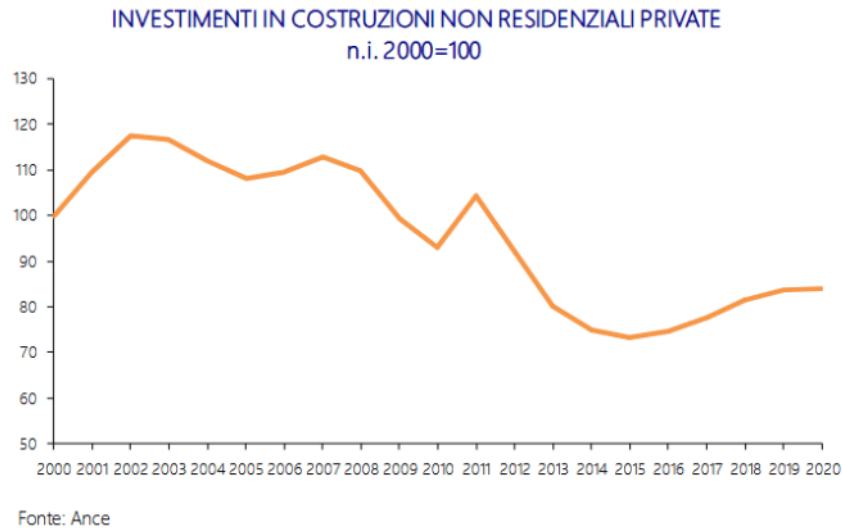


Figura 30: Investimenti in costruzioni non residenziali private

Le previsioni per il 2020

Scenario post crisi

Le costruzioni in Italia rischiano di vedere andare in fumo 34 miliardi di euro di investimenti nel 2020. È questo il risultato della stima preliminare condotta dagli analisti del CRESME sull'impatto settoriale dell'emergenza sanitaria.

In base alle analisi svolte, edilizia e genio civile, includendo investimenti in nuova costruzione e manutenzione straordinaria, potrebbero subire una contrazione **(valutata a valori costanti) del - 22,6% rispetto al 2019**. A titolo di paragone, nel 2009, l'anno più nero per le costruzioni italiane durante la crisi, la flessione degli investimenti era stata del -9,6%.

Va inoltre considerato che prima dell'emergenza sanitaria le costruzioni sperimentavano una fase di crescita che andava consolidandosi; le attese a fine 2019 erano infatti confortanti, con una crescita complessiva del +2,4% (che dava seguito al +3% dell'anno passato), trainata dall'attività nuova costruzione (specialmente in ambito infrastrutturale). Gli investimenti attesi nel 2020, valutati a valori 2019, erano quindi pari a circa 141 miliardi di euro; le stime preliminari del Cresme indicano, invece, che nel 2020 ci si potrebbe fermare ad appena **107 miliardi di euro**, una perdita potenziale, appunto, pari a **34 miliardi di euro**. Se invece si guarda al dato del 2019 (138 miliardi), la caduta è quantificabile in **31 miliardi di euro**.

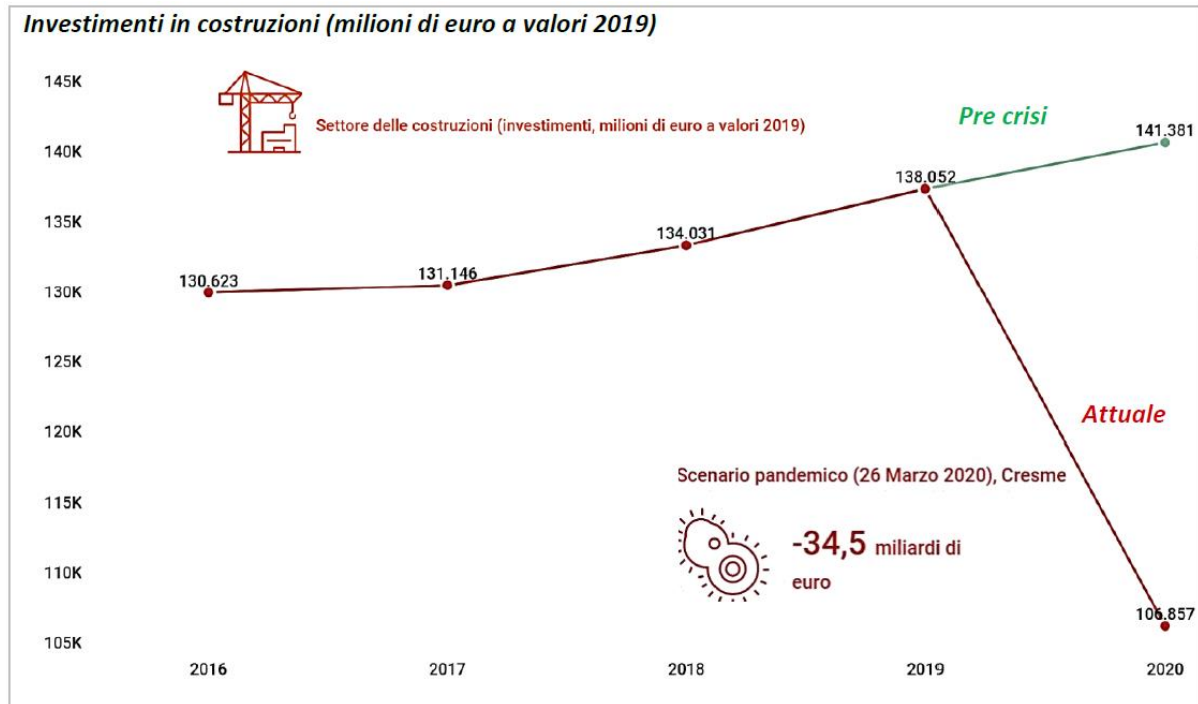


Figura 31: Stime Cresme, CRESME LAB Remote ThinkTank, 26 Marzo 2020 – Mio euro

A livello settoriale, l'impatto sull'attività edilizia coinvolgerebbe in egual misura sia il comparto residenziale sia quello non residenziale (pubblico e privato). Gli investimenti in nuove abitazioni potrebbero crollare di oltre un quinto rispetto al 2019 (-22,6%), mentre più pesante potrebbe essere il blocco dell'attività di ristrutturazione, quantificabile in un -23,5% della spesa. **Il settore residenziale potrebbe quindi perdere, rispetto alle attese di inizio 2020, 3,9 miliardi di nuova costruzione e ben 13,2 miliardi di ristrutturazioni.** Numeri parimenti negativi potrebbero riguardare il settore non residenziale (-23% per la nuova costruzione privata, -27% per la nuova costruzione pubblica, -30% per la riqualificazione in ambito privato e -27% in ambito pubblico), che equivalgono a 3,2 miliardi per il non residenziale nuovo privato (-1,3 miliardi per il pubblico) e 6,8 miliardi per la riqualificazione privata (-1,7 miliardi per quella pubblica). Seppur di minore entità, potrebbe essere drammatico anche il dato sui minori investimenti in opere infrastrutturali, che crollerebbero del -12,6%, sia in ambito di nuova costruzione (-2,5 miliardi), sia in ambito di manutenzione straordinaria (-1,9 miliardi).

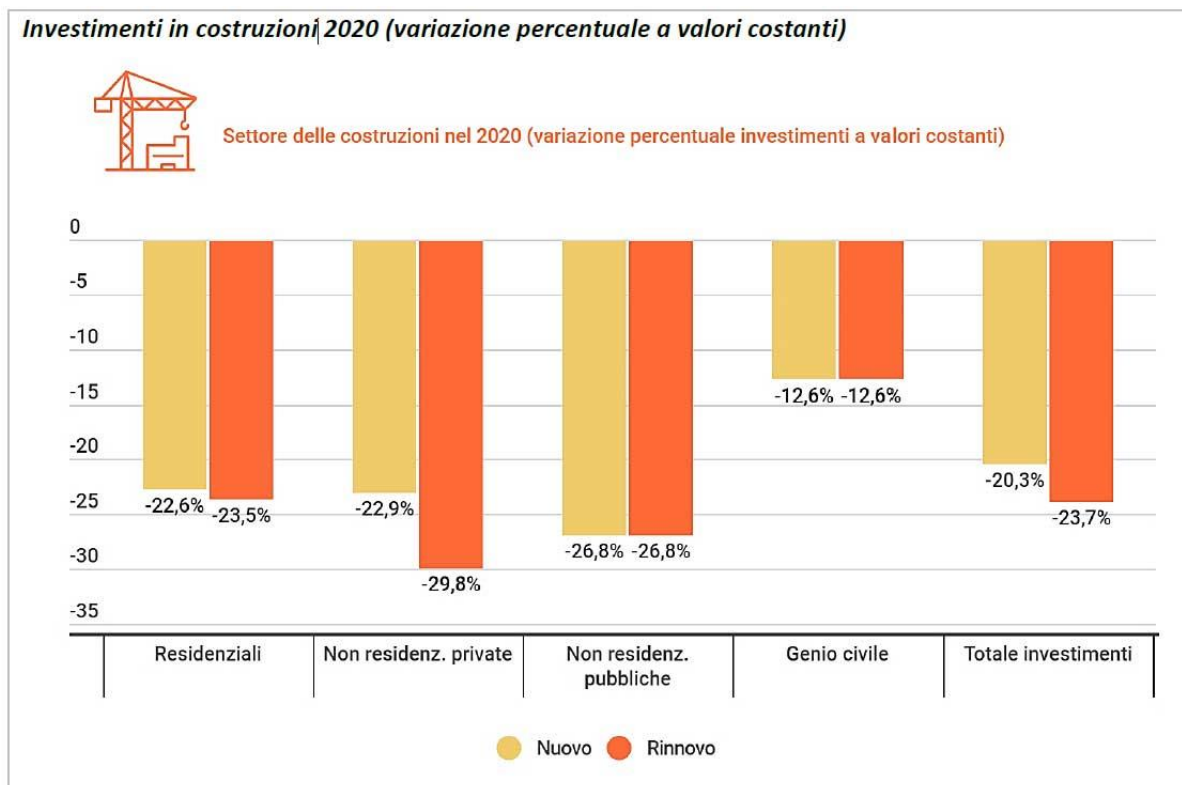


Figura 32: Stime Cresme, CRESME LAB Remote ThinkTank, 26 Marzo 2020 – Variazione percentuale

Alla base di questo scenario vi sono assunzioni sulla entità e sulla durata del blocco dell'attività imposto al settore nel quadro di contenimento dell'epidemia in atto:

- quasi totale sospensione dei cantieri per un trimestre per le nuove costruzioni non di pubblica utilità;
- quasi totale sospensione dei cantieri per un trimestre per gli interventi di riqualificazione edilizia (salvo riparazioni improrogabili, si consideri che nei mesi fra marzo e maggio viene effettuato il 35% degli interventi)
- parziale sospensione dei cantieri per le opere del genio civile di nuova costruzione e di manutenzione straordinaria (ad esclusione infrastrutture strategiche, edilizia sanitaria, ecc.)
- ripartenza improntata alla cautela da giugno a ottobre.

Si tratta di ipotesi in continua evoluzione che, come tali, a mano a mano che la situazione andrà delineandosi, saranno oggetto di revisione nei prossimi mesi.

L'Edificio Digitale: una opportunità di crescita per il settore

Nei capitoli precedenti si è analizzato l'impatto della digitalizzazione e le opportunità derivanti dalla identificazione degli edifici in un ambiente IoT, in termini di maggiore sicurezza, migliore esperienza d'uso dei prodotti e delle tecnologie, di messa a disposizione di nuovi Servizi a valore aggiunto e nuove Applicazioni, rese possibili dai dati prodotti dalle "Cose" interconnesse, che determinano innovative ed aggiuntive fonti di ricavo per gli attori della filiera. E' quindi un fatto che la prospettiva

dell'Edificio 4.0 rappresenti una importante occasione di sviluppo del mercato. Gli ultimi dati dell'Osservatorio Internet of Things del Politecnico di Milano, resi noti ad aprile 2020, evidenziano come il mercato IoT in Italia stia crescendo a ritmi sostenuti, raggiungendo nel 2019 il valore di 6,2 Mld di euro, con un + 24% rispetto al 2018. A spingerlo sono soprattutto gli **Smart Meter** (contatori del gas ed elettrici) e lo **Smart Asset Management**, settori che da soli valgono 1.6 miliardi di euro. Parliamo di **3,2 milioni di contatori smart gas** (il 58% del totale) e di **5,7 milioni di smart meter elettrici** (il 37% di tutti i contatori elettrici) installati nel solo 2019.

Performance interessanti anche per il settore **Smart Car** (1.2 miliardi di euro) e quello degli **Smart Building** (670 milioni). Seguono poi Smart Factory e **Smart Home**, quest'ultimo in crescita del 39,4% rispetto al 2018, grazie anche alla spinta degli assistenti vocali. Ottima anche la crescita del +55% dei piccoli e grandi elettrodomestici smart, sempre rispetto all'anno precedente.

Se l'attenzione ai benefici della digitalizzazione e l'accesso a tecnologie smart è in evidentemente in aumento presso l'utenza, non altrettanto reattivo risulta l'intero sistema delle costruzioni. Il livello tecnologico presente nelle nostre abitazioni e negli edifici italiani è lungi dall'essere adeguato. Eppure tutti gli studi convergono nel sottolineare l'enorme potenziale di crescita economica, laddove gli edifici fossero effettivamente protagonisti del processo di transizione digitale in atto. Boston Consulting Group stimava nel 2018 che l'impiego di nuove applicazioni software e piattaforme digitali potesse portare ad una riduzione del costo totale dell'intero ciclo di vita di un progetto edile di quasi il 20%. Per il settore non residenziale, ad esempio, l'analisi stimava che i risparmi potessero variare dal 13 al 21% nelle fasi di progettazione e costruzione, e dal 10 al 17% nella fase della gestione del patrimonio. Considerando che il settore delle costruzioni, secondo l'Istat, sostiene una spesa per l'acquisto di beni e servizi finalizzati alla costruzione di fabbricati residenziali e non residenziali di circa **170 miliardi di euro**, quantificando la riduzione di costo partendo dai dati di contabilità nazionale dell'Istat e applicando le percentuali previste da Boston Consulting Group, si arriverebbe a stimare un risparmio annuale compreso tra i **20,4 e i 32,2 miliardi di euro** derivato dall'utilizzo della digitalizzazione nelle fasi di progettazione e di costruzione. Risparmi che si tradurrebbero in **maggiori investimenti** nel settore, **aumento dell'occupazione**, opere di qualità a costi contenuti.

Appendice

Criteri di classificazione degli edifici

Relazione tra classificazione e valore

In attesa che venga proposto e codificato uno standard europeo è possibile ipotizzare una prima fase in cui la classificazione sia definita su base volontaria, tenendo conto dei parametri e delle caratteristiche che vengono illustrate qui di seguito. Per cominciare la classificazione dovrà distinguere tra i vari tipi di edificio: residenziale e non-residenziale

Edifici residenziali	Edifici non residenziali
Edifici monofamiliari	Edifici pubblici/istruzione (scuole, biblioteche, etc.)
Edifici plurifamiliari	Edifici commerciali (uffici, negozi, etc.)
	Edifici pubblici/sanità (ospedali, case di riposo, etc.)
	Ospitalità (alberghi, ristoranti, B&B, etc.)

Tabella 3: Tipologie di edificio

La classificazione dovrà considerare il livello di automazione e la disponibilità sul Cloud dei dati relativi all'edificio in questione, rispetto ad alcuni domini:

Energia	Sicurezza	Ambiente
Riscaldamento	Sistemi di allarme (antintrusione volumetrico, etc.)	Illuminazione
Raffrescamento	Sistemi di rilevazione (incendio, allagamento, fughe di gas, black-out energetici, etc.)	Parametri ambientali (temperatura, umidità, irraggiamento, etc.)
Elettrodomestici		Prestazioni dell'involucro
Produzione energia da fonti rinnovabili		
Immagazzinamento energia elettrica (storage) e e-mobility		

Tabella 4: Domini di valutazione

La classificazione dovrà riguardare inoltre le modalità di connessione al Cloud:

- Tipo di comunicazione: tramite radio (WLAN), cavo (LAN), ecc.

- Disponibilità di comunicazione in assenza di alimentazione principale: esiste o meno un canale secondario di comunicazione nel caso il canale principale sia indisponibile?
- Caratteristica della comunicazione: monodirezionale o bidirezionale?

Questo è uno dei modi di descrivere il livello di “smartness” e altri se ne possono trovare, per esempio classificando il livello di “smartness” dell’edificio a partire dai casi d’uso abilitabili, descritti qui di seguito, e in funzione di quanti e quali casi d’uso è possibile gestire usando le infrastrutture di comunicazione e i dispositivi IoT presenti nell’edificio. L’incredibile mole di dati ⁵⁹ che un complesso sistema di automazione di un edificio può generare rappresenta un notevole patrimonio per tutti gli attori della filiera.

Qui di seguito, infine, alcuni spunti utili per capire come trarre valore da queste sequenze di bit che possono essere intelligentemente tradotte in fonte di ricavi e/o di riduzione di costi per i vari attori:

1. Migliorare i prodotti

Uno dei principali benefici ottenibili tramite le applicazioni IoT è rappresentato dall’opportunità che hanno le aziende produttrici di analizzare approfonditamente le modalità di utilizzo dei propri dispositivi e sistemi; in tal modo è possibile decidere se, e soprattutto come, sviluppare le nuove generazioni di prodotto al fine di razionalizzare ed ottimizzare/focalizzare gli investimenti. Un banale esempio è lo studio del comportamento d’uso dei prodotti, ovvero studiando come viene usato un impianto domestico si potrebbe arrivare alla conclusione che non ha senso implementare una data funzione o le funzioni nel dispositivo supervisore principale visto che, studiando le abitudini d’uso degli utilizzatori, si potrebbe capire che tale funzione non viene mai utilizzata direttamente dal touch screen del supervisore, ma solamente da App installata in uno Smartphone o in un Tablet. In tal caso l’azienda produttrice, raccogliendo le informazioni dal campo, potrebbe decidere di non implementare tale funzione nella nuova generazione di touch screen, se non addirittura eliminare il touch screen di supervisione per concentrare gli sforzi solamente nell’App per dispositivi mobili.

2. Personalizzare i prodotti

Un’ulteriore ricaduta positiva legata alla raccolta dei dati generati dai prodotti e dai sistemi connessi è la possibilità di creare soluzioni personalizzate utili per soddisfare le esigenze specifiche di particolari segmenti di clientela, riuscendo quindi a differenziarsi dalla concorrenza in modo efficace. Solamente conoscendo i comportamenti, i gusti e le misure delle persone risulta possibile cucire un vestito fatto ad hoc per ognuna di esse. Più dati riceviamo dai nostri clienti più siamo in grado di personalizzare prodotti e servizi, soprattutto se questi ultimi possono essere erogati in automatico dal Cloud tramite le App, aumentando così sia la soddisfazione che la fidelizzazione del cliente.

⁵⁹ Questi dati sono soggetti ovviamente alle norme sulla privacy e di questi aspetti così come delle regolamentazioni del loro utilizzo verranno trattate nel capitolo **Errore. L'origine riferimento non è stata trovata..** Per il momento si assuma che tutto quello che verrà descritto sia compatibile, come vedremo, con tali norme.

3. Offrire servizi

Indubbiamente uno dei principali vantaggi del paradigma IoT è rappresentato dalla possibilità di offrire ai clienti dei servizi abbinati alla vendita del prodotto. I servizi possono spaziare da contratti di manutenzione remota (l'installatore può vedere da remoto o addirittura in anticipo la rottura di un prodotto senza bisogno di sopralluogo, riducendo i costi e velocizzando la riparazione), alla teleassistenza e telemedicina, alla vendita di pacchetti di assistenza alla persona (dai giovani agli anziani, dai degenti fino alle persone diversamente abili). Si può continuare con polizze assicurative più economiche o personalizzate, per arrivare infine ai servizi di monitoraggio dei consumi di acqua, luce e gas e quindi di consulenza per l'efficientamento energetico degli edifici nonché servizi di gestione remota di alcune utili funzioni quali per esempio l'irrigazione (con impostazione automatica dei programmi di irrigazione in base ai fabbisogni stagionali e alle previsioni meteo) o la gestione dei carichi (con controllo da remoto delle politiche di utilizzo dei flussi energetici in base alle tariffe, all'insolazione diurna e/o alla presenza delle persone nell'edificio).

4. Ottimizzare i processi

Oltre al valore che l'IoT può potenzialmente portare sul mercato, c'è una considerazione da fare relativamente ai benefici interni aziendali derivati dall'ottimizzazione dei processi produttivi e distributivi. L'aumento dell'efficienza di tutto il ciclo produttivo, misurabile come riduzione dei tempi e dei costi manifatturieri, maggiore flessibilità nella produzione di piccoli lotti personalizzati, l'analisi in real-time delle difettosità e la gestione efficace dei rientri/riparazioni, incide direttamente sulla qualità del prodotto e del servizio erogato dall'azienda.

5. Vendere i dati a terzi

Una possibile fonte di ricavi per le aziende operanti nel mercato IoT è rappresentata dalla cessione dei dati di utilizzo e funzionamento dei dispositivi connessi ad aziende interessate a tale dato per fini differenti rispetto a quelli per i quali il prodotto è stato acquistato.

6. Cross selling

Un ottimo modo per generare ritorni economici dalla connettività dei prodotti IoT è lo sfruttamento del canale di comunicazione con l'utente finale offerto dalle App e dagli eventuali display di tali prodotti/sistemi (per esempio un Videocitofono). Attraverso questi canali di comunicazione è infatti possibile informare l'utente di novità di prodotto e/o miglioramenti del prodotto già acquistato e/o del servizio, sia in modo massivo (stessa comunicazione a tutti i clienti utilizzatori) che in modo mirato (diversa comunicazione in base agli usi e abitudini di specifici cluster di clienti).

Esempi di classificazione degli edifici

Una proposta operativa

Un possibile esempio di classificazione degli edifici potrebbe prevedere due codici numerici (SRlXX): il primo dei quali si riferisce al numero di domini di automazione e di connessione al Cloud presenti nell'edificio ed il secondo relativo alle caratteristiche del canale di comunicazione:

Prima cifra

1. un dominio gestito (energia, sicurezza o ambiente)
2. due domini gestiti
3. tre domini gestiti

Seconda cifra

1. connessione monodirezionale senza canale di backup
2. connessione bidirezionale senza canale di backup
3. connessione bidirezionale con canale di backup

Un altro possibile criterio di classificazione è in base ai casi d'uso; con questa metodologia il codice numerico è uno solo e rappresenta direttamente il numero di casi d'uso implementati.

Esempio di classificazione con codice a due cifre

SRl21 = edificio con connessione diretta al Cloud per la gestione di sensori di 2 diversi domini (energia, sicurezza e/o ambiente) ma senza un canale di comunicazione alternativo e senza possibilità di inviare comandi all'edificio stesso

SRl33 = edificio con i 3 domini connessi sia con sensori che attuatori e con connessione bidirezionale e con canale di backup

Esempio di classificazione con codice a una cifra

SRl2 = edificio con 2 casi d'uso implementati

Invece, nel caso dei dispositivi IoT, un possibile esempio di classificazione considera due codici numerici (IoTXX), il primo dei quali riferito al tipo di dispositivo ed il secondo al grado di autonomia e connettività:

prima cifra

1. sensore o attuatore
2. sensore e attuatore

seconda cifra

1. bassa autonomia e Cloud proprietario
2. alta autonomia e dati disponibili per Cloud di terze parti, interoperabilità tra i dispositivi di produttori diversi e tra i rispettivi Cloud

Esempio di classificazione per dispositivo IoT

IOT21 = dispositivo con attuatore e sensore con connessione a Cloud proprietario

IOT12 = sensore con connessione a Cloud condiviso

Sempre per quanto riguarda la classificazione degli edifici, in ambito europeo proseguono i lavori per definire una metodologia di calcolo dell'SRI – Smart Readness Indicator – parametro destinato ad identificare la capacità dell'edificio o della singola unità abitativa ad adattarsi alle esigenze degli utenti, ad ottimizzare la sua performance energetica e prestazione generale, ad interagire in maniera efficace con i segnali delle reti collegate.



Figura 33: Smart Readness Indicator

La discussione su come classificare digitalmente un edificio è ancora molto aperta. Allo stesso modo sarà necessario capire se opportuno definire distinti indicatori in caso di edifici residenziali e non, o tra edifici oggetto di ristrutturazione e nuove costruzioni. Un altro aspetto da chiarire sarà quando deve essere classificato l'edificio, se al momento della compravendita o della stipula del contratto di locazione, oppure direttamente al termine della costruzione o ristrutturazione, oppure semplicemente su base volontaria.

Tassonomia degli elementi di un'architettura IoT

Di seguito viene illustrata la descrizione di architettura IoT disaccoppiata dove, su ogni singolo layer, sono esplose le diverse funzionalità.

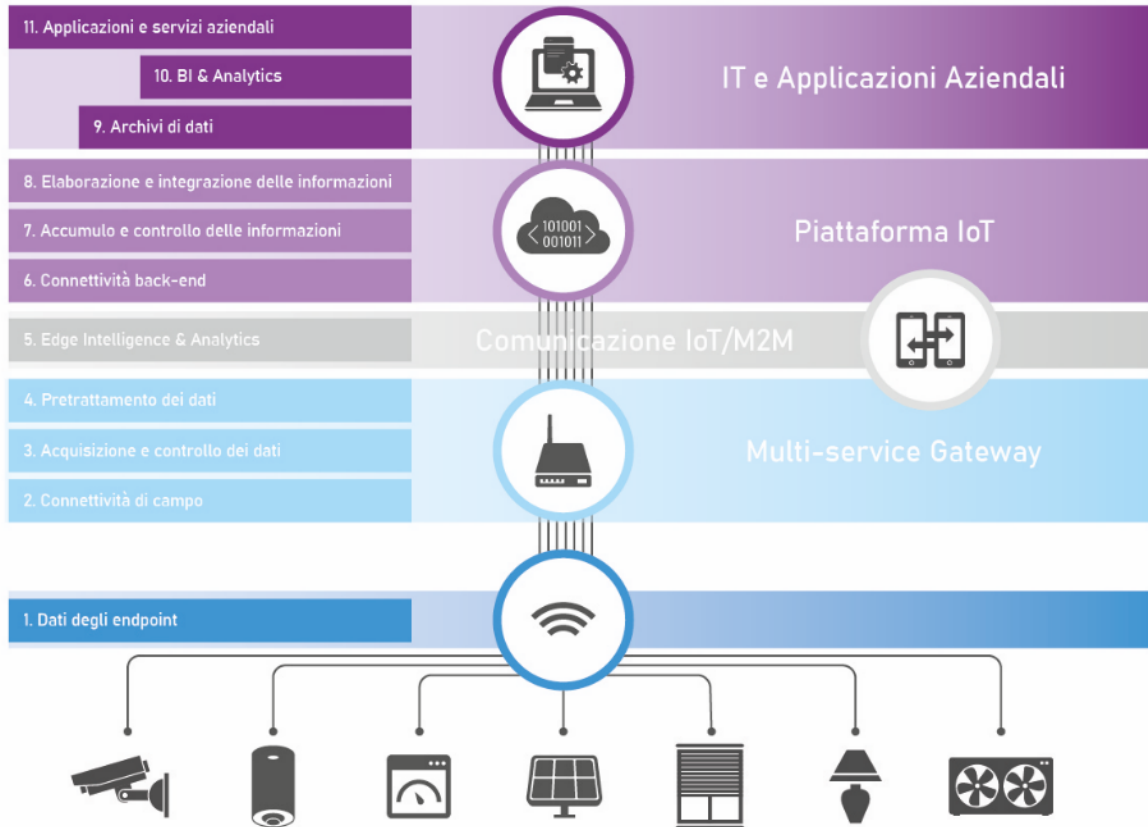


Figura 34: IoT Functional Taxonomy

La matrice qui sotto riporta invece la IoT Functional Taxonomy dei diversi building blocks che caratterizzano i middleware on the Edge, i microservizi Cloud, le piattaforme di integrazione IoT e le enterprise IoT platform. I vari building blocks sono funzionali per capire quanto esposto nei seguenti paragrafi.

FP	Field Protocols	C	Connection
AM	Application Management	A	Application
DB	Database, Data Store	AI	Application IF, Rules Engine
DA	Device Abstraction	BI	Business Intelligence
DM	Device Management	MR	Message Routing, Broker
Secutiry	Secutiry	AN	Analytics
VPN	VPN	HM	Health Management
		SA	Security Access, RBAC
		EI	Enterprise Integration

Figura 35: Building Blocks Taxonomy

Brown Field e Green Field in architetture IoT

Riprendendo il concetto di multi-service gateway e software gateway, si possono ipotizzare i seguenti scenari architetturali che trovano espressione rispettivamente in applicazioni di retrofitting (brown field) o di green field.

Nel primo caso vengono inseriti gateway fisici a livello campo, i multi-service gateway, per l'interfacciamento al mondo legacy, oppure gateway virtuali a livello Cloud (tipicamente micro-servizi) per l'interfacciamento e la normalizzazione di oggetti già dotati di connettività; in entrambi i casi l'integrazione viene demandata ai System Integrator. Nella figura che segue l'elemento centrale (aggregation level) può essere infatti presente come gateway fisico (spostato a sinistra verso il campo) o gateway virtuale (micro-servizio pluggabile più a destra verso il Cloud).

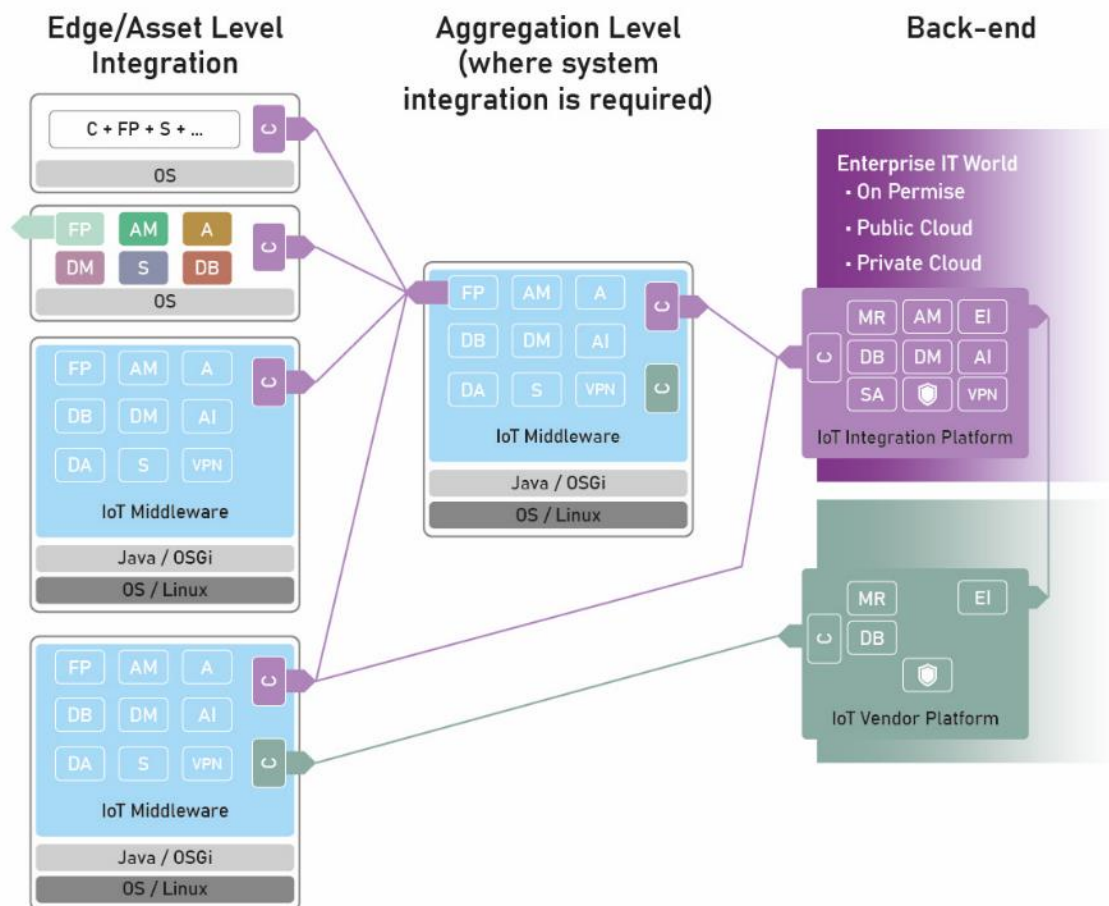


Figura 36: Taxonomy di un Architettura Brown Field

Nel secondo caso è più comune che gli oggetti siano già smart e possano esporre API a livello Edge o livello Cloud per offrire nativamente differenti possibilità di integrazione.

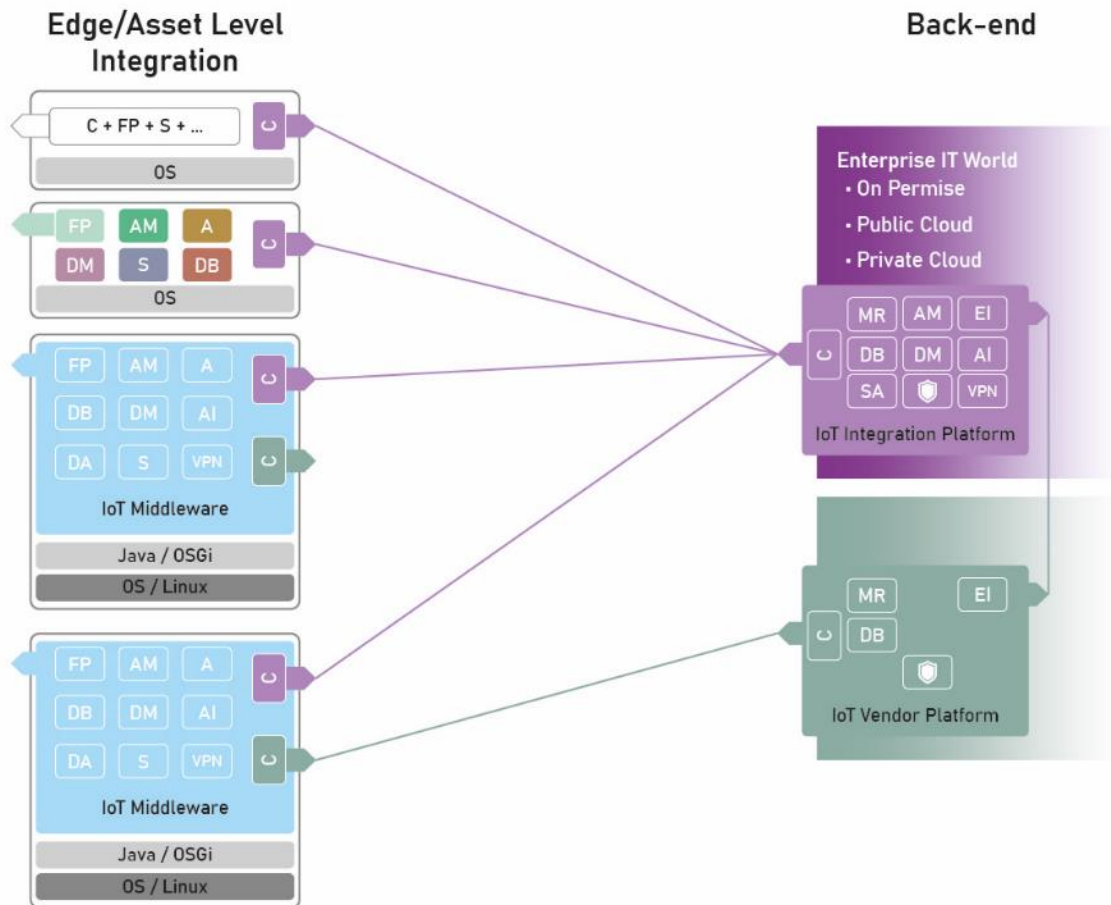


Figura 37: Taxonomy di un Architettura Green Field

In entrambi i casi si rende essenziale lo strato di Platform dove si possa gestire in sicurezza il routing direzionale dei messaggi di telemetria, l'integrazione Cloud-to-Cloud a livello di back-end e l'orchestrazione degli aggiornamenti e cambi di configurazione.

Gestione dei modelli di AI sul campo in architetture IoT

Il seguente schema riprende il concetto di disaccoppiamento degli strati campo ottenuto grazie alla Piattaforma IoT evidenziando come per orchestrare intelligenza distribuita siano necessari, oltre a multi-service IoT gateways, un framework on the Edge ed una sua controparte centrale di gestione remota, la Piattaforma IoT. In questo modo si possono gestire i dispositivi e le applicazioni su campo, la sicurezza, l'integrazione verso Business Applications e Analytics.

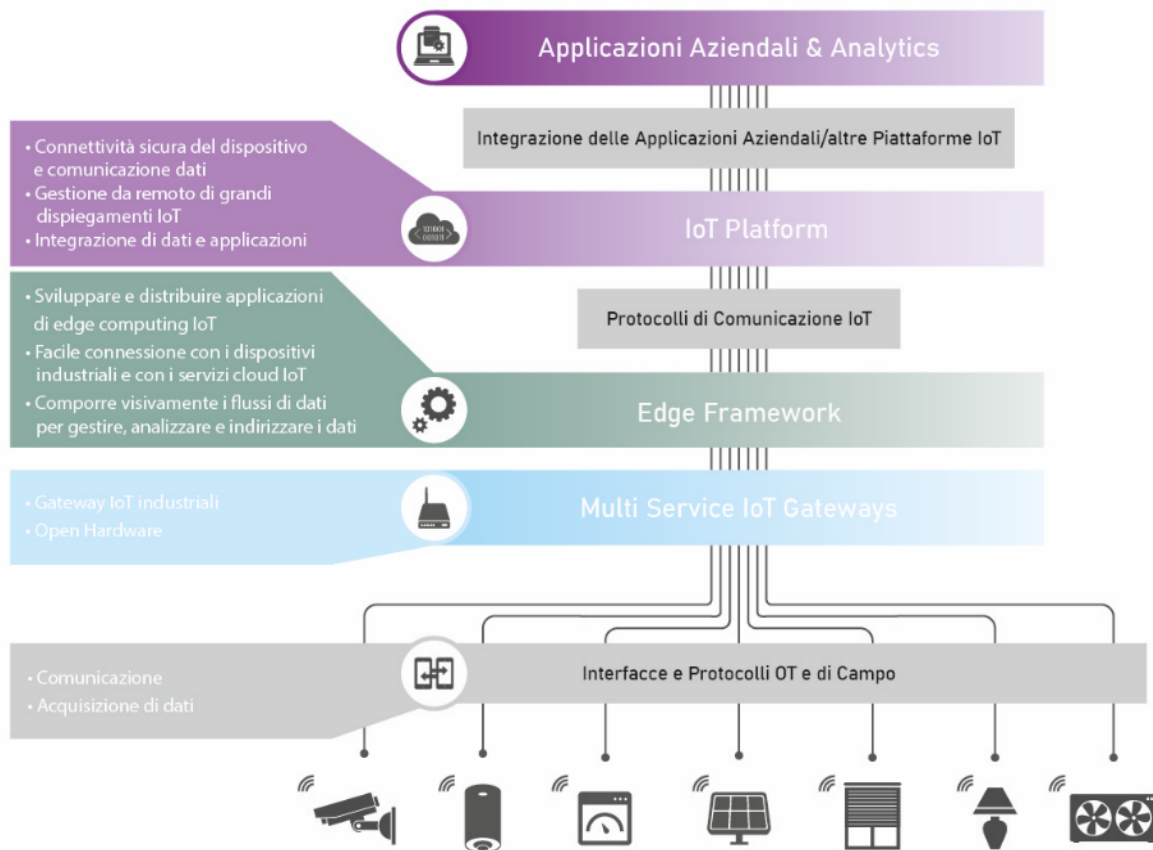


Figura 38: Architettura IoT disaccoppiata

Facendo riferimento a quanto sopra i dispositivi di campo, ormai sempre più performanti, sono in grado di elaborare in locale (on the Edge) quanto ricevuto da sensori e frazionare quella parte di analitiche che alleggerisce ciò che diversamente dovrebbe essere fatto esclusivamente a livello Cloud. In questo modo si riescono a trasferire dati/informazioni pre-processate direttamente in locale e ridurre le latenze ed i costi di trasmissione verso il Cloud qualora necessario.

Lo stesso concetto può essere applicato laddove le analytics on the Edge siano rappresentate da un algoritmo/modello precedentemente addestrato a livello Cloud che gira nei multi-service gateways portando l'intelligenza artificiale (AI) direttamente sul campo. Si tratta di modelli inferenziali.

Vien da sé che, per orchestrare un tale livello di intelligenza distribuita in maniera dinamica, sia necessario lo strato centrale precedentemente definito come IoT Platform. È proprio attraverso quest'ultimo che fluiscono i dati di campo andando ad alimentare gli algoritmi di deep learning e machine learning dove viene addestrato ed affinato il modello di AI. Una volta completato, il

modello può essere deployato automaticamente sui gateways attraverso l'IoT Platform, che si occupa del trasferimento in sicurezza, della verifica di integrità e del censimento delle operazioni.

Attraverso iterazioni successive il processo si ripete ed il modello si affina nel tempo.

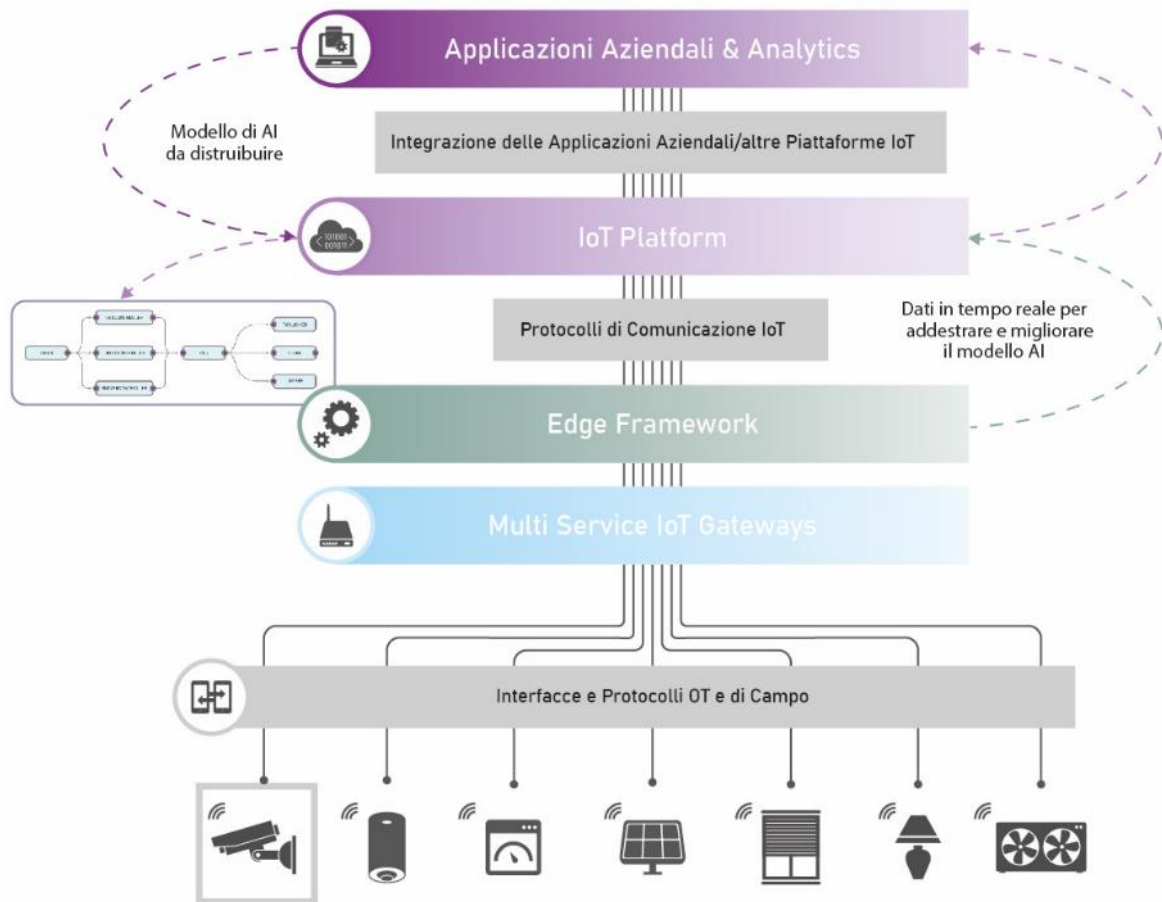


Figura 39: Il concetto di AI centralizzata su Cloud o distribuita a livello Edge

Indice delle Fonti

- “Apache Hadoop” - <http://hadoop.apache.org/>
- “Apache Hadoop Tutorial” - https://hadoop.apache.org/docs/r1.2.1/mapred_tutorial.html
- “CSA Launches New Security Guidance for Early Adopters of the IoT” - <https://Cloudsecurityalliance.org/media/news/csa-launches-new-security-guidance-for-early-adopters-of-the-iot>
- “Design Principles for Industrie 4.0 Scenarios” - <https://ieeexplore.ieee.org/document/7427673/authors>
- “Development of an Assessment Model for Industry 4.0: Industry 4.0-MM ” - https://www.researchgate.net/publication/319640255_Development_of_an_Assessment_Model_for_Industry_40_Industry_40-MM?_sg=B8W-kJgkTGQZ8E0n_UPgYOcmup12Cj0WCmR5N4uHor-58MJZn2clBA_TVz5PctegWU4hD7H_f5rE_FgD52rhUL5QghWAYRkhw
- “Digital Twins vs. Building Information Modeling (BIM)” - <https://www.iotforall.com/digital-twin-vs-bim/>
- European Commission: Building a European data economy
- European Political Strategy Centre (EPSC): Enter the Data Economy
- Forbes: Uber the big data economy
- “Gartner IT Glossary > Internet of Things (IoT)” - <https://www.gartner.com/it-glossary/internet-of-things>
- GDPR
- “Germany: Industrie 4.0 – Digital Transformation Monitor – Report (European Commission)” - https://ec.europa.eu/growth/tools-databases/dem/monitor/sites/default/files/DTM_Industrie%204.0.pdf
- “Global Mobile Data Traffic Forecast” - <https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/mobile-white-paper-c11-520862.html>
- Harvard Business Review: Big Data The Management Revolution
- “Il Quarto Paradigma” - <https://www.scienzainrete.it/contenuto/articolo/quarto-paradigma>
- Il regolamento 679/2016, G.U.U.E. n. L 119 del 4 maggio 2016
- Il Sole 24 Ore: Raccolta, elaborazione e utilizzo delle informazioni in rete sono il petrolio del futuro
- “IoT Standards and Protocols” - <https://www.postscapes.com/internet-of-things-protocols/>
- “ISTAT, INDICATORI DEMOGRAFICI” - <https://www.istat.it/it/archivio/180494>
- “ITU-T Recommendations” - <http://www.itu.int/itu-t/recommendations/rec.aspx?rec=Y.2060>
- “Kevin Ashton Biography” - http://ethw.org/Kevin_Ashton
- “Kevin Ashton Describes “the Internet of Things”” - <https://www.smithsonianmag.com/innovation/kevin-ashton-describes-the-internet-of-things-180953749/>
- Key4biz: Unicorn, le 193 startup che superano \$ 1 miliardo. Uber al primo posto vale 68 miliardi
- “M2M” - https://en.wikipedia.org/wiki/Machine_to_machine
- McKinsey: Monetizing car data New service business opportunities to create new customer benefits
- “Mobile cellular subscriptions ” - <https://data.worldbank.org/indicator/IT.CEL.SETS.P2?end=2016&start=1981>
- “Moore's law” - https://en.wikipedia.org/wiki/Moore%27s_law
- “Origins of the Digital Twin Concept” - https://www.researchgate.net/publication/307509727_Origins_of_the_Digital_Twin_Concept

- “Platform Business Model” - <https://www.applicoinc.com/blog/what-is-a-platform-business-model/>
- Product Lifecycle Management: Driving the Next Generation of Lean Thinking, 2005 by Michael Grieves
- “Pronta la proposta di legge sulla sharing economy” - <http://www.techeconomy.it/2016/03/02/pronta-la-proposta-legge-sulla-sharing-economy/>
- “READY 2 SERVICES” - <https://www.smartbuildingsalliance.org/project/ready-2-services/>
- “Representational state transfer” - https://en.wikipedia.org/wiki/Representational_state_transfer
- “Security Guidance for Early Adopters of the Internet of Things (IoT))” - https://downloads.Cloudsecurityalliance.org/whitepapers/Security_Guidance_for_Early_Adopters_of_the_Internet_of_Things.pdf
- “Sharing Economy e Modelli Organizzativi” - http://tesi.cab.unipd.it/53193/1/Landini_Alessandro.pdf
- “Smart Readiness Indicator for Buildings” - <https://smartreadinessindicator.eu>
- “The 2017-2022 App Economy Forecast” - <https://www.appannie.com/en/insights/market-data/app-annie-2017-2022-forecast/>
- “The App Economy Forecast” - <https://www.appannie.com/en/insights/market-data/app-economy-forecast-6-trillion-market-making/>
- “The App Economy Forecast” - <https://www.appannie.com/en/insights/market-data/app-annie-2017-2022-forecast/>
- The Economist: Data is giving rise to a new economy
- “The Industrial Internet Consortium’s Security Working Group” - <http://www.iiconsortium.org/wc-security.htm>
- “Toast of the IoT: The 1990 Interop Internet Toaster” - <https://ieeexplore.ieee.org/document/7786805/>
- “Unsupervised learning” - https://en.wikipedia.org/wiki/Unsupervised_learning
- “When Things Start to Think” - <https://dl.acm.org/citation.cfm?id=519271>

Indice delle Figure

Figura 1: Il primo tostapane connesso	10
Figura 2: La legge di Moore	11
Figura 3: Cisco Visual Networking Index 2017	12
Figura 4: Source: Cisco Annual Internet Report, 2018–2023	13
Figura 5: Crescita connessioni M2M per segmenti applicativi	13
Figura 6: LPW/PAN (Low Power Wide Peripheral Area Network)	14
Figura 7: Data Silos	16
Figura 8: Data Lake	17
Figura 9: “Cose” connesse e non nel green e brown field	18
Figura 10: Embedded Computer e Gateway	21
Figura 11: Gateway ed Edge Computer	21
Figura 12: IaaS, PaaS e SaaS	22
Figura 13: Industry 4.0 e le precedenti rivoluzioni industriali	25
Figura 14: Spazio reale e virtuale	28
Figura 15: Il concetto di Digital Twin e Asset	29
Figura 16: Le principali categorie di dati da monetizzare	32
Figura 17: Catena di valore nella generazione dei dati	34
Tabella 1: Benefici e rischi/colli di bottiglia per tipologia di attore	34
Figura 18: La transizione del Valore da Prodotto a Servizio abilitata dall’IoT	37
Figura 19: Tecnologie disruptive per il mercato tradizionale delle auto	39
Tabella 2: Livello di sensibilità della privacy percepita dal cliente per categorie di dati	40
Figura 20: Componenti funzionali di un gateway IoT	48
Figura 21: Suddivisione in sottoinsiemi di una architettura IoT	50
Figura 22: Componenti funzionali di una piattaforma IoT	50
Figura 23: BIM vs IoT	53
Figura 24: Flussi di dati ed energia	58
Figura 25: Relazioni tra elettrodomestici e consumi	61
Figura 26: La struttura dell’SRI	70
Figura 27: La struttura del R2S	70
Figura 28: La sicurezza in ambito IoT	73
Figura 29: Investimenti in abitazioni	85
Figura 30: Investimenti in costruzioni non residenziali private	86
Figura 31: Stime Cresme, CRESME LAB Remote ThinkTank, 26 Marzo 2020 – Mio euro	87
Figura 32: Stime Cresme, CRESME LAB Remote ThinkTank, 26 Marzo 2020 – Variazione percentuale	88
Tabella 3: Tipologie di edificio	90
Tabella 4: Domini di valutazione	90
Figura 33: Smart Readiness Indicator	94
Figura 34: IoT Functional Taxonomy	95
Figura 35: Building Blocks Taxonomy	95
Figura 36: Taxonomy di un Architettura Brown Field	96
Figura 37: Taxonomy di un Architettura Green Field	97
Figura 38: Architettura IoT disaccoppiata	98
Figura 39: Il concetto di AI centralizzata su Cloud o distribuita a livello Edge	99

Indice delle Tabelle

Tabella 1: Benefici e rischi/colli di bottiglia per tipologia di attore.....	34
Tabella 2: Livello di sensibilità della privacy percepita dal cliente per categorie di dati	40
Tabella 3: Tipologie di edificio	90
Tabella 4: Domini di valutazione	90