DIGITAL FUTURE
OR12 – Definizione della Piattaforma di Telemedicina

Analisi di metodologie e standard in ambito IoT per la sanità

TR12.2

AUTORE: EXPRIVIA S.P.A

UNIONE EUROPEA
FONDO EUROPEO DI SVILUPPO REGIONALE

Ministero Sviluppo Economico

REGIONE PUGLIA
AREA POLITICHE PER LO SVILUPPO ECONOMICO
IL LAVORO E L'INNOVAZIONE

Regolamento regionale della Puglia per gli aiuti in esenzione n. 17 del 30/09/2014

Titolo II – Capo 1 "Aiuti ai programmi di investimento delle Grandi Imprese"

POR PUGLIA FESR 2014 – 2020

CONTRATTO DI PROGRAMMA

"Digital Future"

CODICE PROGETTO: CP12PA6

1. Indice dei contenuti

2. Premessa

Il presente Report è la sintesi rielaborata, emendata, arricchita di riferimenti, anche in margine, e del glossario del Documento "**IoT Reference Architetture"** realizzato dal **Comitato IoT,** attivato dalla associazione imprenditoriale "**Confindustria Digitale**" nel periodo 2015 – 2016. Exprivia ha contribuito ai lavori dedicandosi alla analisi ed elencazione degli standard tecnici di riferimento.

Il Report non ha la pretesa di essere esaustivo nella rappresentazione del complesso delle tecnologie che sono alla base dell'Internet of Things, tuttora soggette ad una continua evoluzione; ne propone una analisi di alto livello: dai devices ai protocolli e reti di comunicazione a corto e lungo raggio. Sono inoltre accennati i contenuti dei layer sovrastanti, così come rappresentati nel tipico stack ISO/OSI.

Le rappresentazioni architetturali che meglio descrivono la complessità e la variabilità del mondo IoT sono state probabilmente proposte dagli Enti ISO/IEC e AIOTI: i quali sottolineano sia la necessità di una layer intermedio (edge layer) tra i dispositivi e la rete estesa sia la necessità di affrontare il tema della sicurezza secondo il principio "by design", articolandone l'analisi (con la relativa risoluzione) su ogni stack ed elemento della architettura. Nel Report si propone principalmente l'analisi del contributo offerto da ITU-T (International Telecommunication Union – T workgroup) in quanto comprensivo dei lavori citati e di più semplice illustrazione. Sono accennate le promettenti tecnologie Long Range non licenziate, il ruolo di alcuni dei protocolli di comunicazione; sono proposte specifiche riflessioni sulle architetture dell'application layer e riportati nei diversi capitoli, in tabelle di sintesi, gli enti e i documenti relativi agli standard di riferimento.

3. Introduzione

Cosa è l'Internet delle cose o Internet of things?

Un sintetica descrizione fu proposta nel 2015 dallo IERC.

"IoT is a dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual "things" have identities, physical attributes, and virtual personalities and use intelligent interfaces, and are seamlessly integrated into the information network".

Ovvero, in italiano:

" *l'IoT può essere definito come una infrastruttura di rete globale con capacità di auto configurazione; basata su protocolli di comunicazione standard e interoperabili, dove gli oggetti fisici e virtuali hanno un'identità, attributi fisici, personalità virtuale e utilizzano interfacce intelligenti, oltre ad essere perfettamente integrati nella rete info-telematica*".

L'Internet of Things è una realtà in continua evoluzione, con sempre nuovi ambiti applicativi e modelli di connettività: basati sullo sviluppo delle applicazioni e della loro interoperabilità; supportati dalla definizione di una comune semantica e dalla realizzazione di oggetti sempre più intelligenti, avanzati e performanti. Vi sono poi temi da esplorare, che richiederanno un comune sforzo per la loro definizione e risoluzione. Essi sono resi ancor più complessi dall'elevato numero di standard tecnologici in competizione: sia sui domini applicativi verticali sia sui domini orizzontali. A questi si aggiunge la carenza di business model e dei business case di riferimento, la relativa diffusione delle esperienze, la incertezza sulla profondità ed estensione degli impatti sociali che deriveranno dalla massiccia applicazione dell'internet delle cose.

Si stima che entro il 2020 gli oggetti connessi saranno circa 50 miliardi in tutto il mondo, il traffico dei dati supererà gli 1,6 Zettabyte e lo sforzo di tutti gli operatori delle telecomunicazioni, come pure dei nuovi gestori di servizi IoT, sarà quello di sviluppare soluzioni di connessione di rete per consentire l'interazione con tali oggetti, al fine di ottenere informazioni o modificarne il funzionamento, nel rispetto della sicurezza e della privacy.

Perché ciò sia possibile c'è molto fermento sul fronte degli standard tecnologici, al lavoro delle Organizzazioni ufficiali di Standardizzazione (SDO – Standard Developing Organization) si è affiancato il contributo straordinario di un'ampia tipologia di organismi associativi, consortili, pubblici o privati; finalizzati alla produzione di standard, alla creazione di ecosistemi di

sviluppatori e di soluzioni Open Software. È questo il caso dei consorzi nati a supporto della diffusione di due tecnologie come Zigbee o Bluetooth o dei gruppi di interessi collegati ad una ancora più ampia applicazione di tecnologie già dominanti, come la WI-Fi Alliance e la IPSO Alliance, quest'ultima nata a "promozione" dell'Internet Protocol nel mondo IoT.

Al febbraio 2016, i principali 9 enti di standardizzazione avevano prodotto nel dominio IoT 418 standard, di cui 278 dedicati alle architetture ICT.

Nelle tabelle che seguono sono elencati gli organismi, ufficiali e non, deputati alla standardizzazione tecnica. Rispetto ad altre suddivisioni, orientate agli ambiti applicativi, si propone una suddivisione basata sul contributo offerto nella standardizzazione, funzionale alla implementazione di standard dedicati ad uno o più dei 7 stacks della classica suddivisione ISO/OSI. Per ulteriore semplificazione i contributi sono aggregati nei due macro ambiti architetturali dei layer "fisico/networking" e "services/application". Le iniziative che propongono regole nei domini della security, delle ontologie e della interoperabilità sono elencate nei paragrafi dedicati.

La suddivisione dei contributi prodotti è basata sulla rilevanza e la numerosità degli stessi rispetto al macro-dominio applicativo. Non sono stati considerati i contributi relativi alle connessioni wired o alle RFID; così come non sono da escludere interventi di standardizzazione agenti su più layers degli stack architetturali.

Tabella 1 Official Standard Organization: contributi alla standardizzazione

Official Standard Organization	Web Site	Standard	
		Device - Network Layer	Service - Application Layer
CEN - Comitato Europeo di Normazione	www.cen.eu	●	●
CENELEC - European Committe for Electrotechnical Standardization	www.cenelec.eu	●	
ETSI - European Telecommunications Standards Institute	www.etsi.org	●	●
IEEE - Institute of Electric and Electronic Engineer	www.ieee.org	●	●
IEC - International Electrotechnical Commission	www.iec.org	●	●
IETF - The Internet Engineering Task Force	www.ietf.org	●	●
ISO - International Organization for Standardization	www.iso.org	●	●
ITU-T - International Telecommunication United Nation	www.itu.org	●	●
oneM2M	www.onem2m.org	●	

Per dare ordine al settore, per favorire il dialogo tra i diversi attori, in considerazione del comune obiettivo di garantire un governo della evoluzione tecnologica e al fine di realizzare in Europa un unico Ecosistema IoT di riferimento, un ruolo decisivo è stato assegnato alle Standard Organizations. Allo scopo, nel marzo del 2015, la Commissione Europea ha sostenuto la costituzione della l'AIOTI: l'Alleanza per l'Internet of Things[1].

1 http://www.aioti.eu/#!/page_SPLASH

Tabella 2 Non Official Standard Organization: contributi alla standardizzazione

Non-Official Standard Organization	Web Site	Standard	
		Device - Network Layer	Service - Application Layer
AIOTI - Alliance for Internet of Things Innovation	https://ec.europa.eu/digital-agenda/en/alliance-internet-things-innovation-aioti	●	●
AllSeen Alliance	https://allseenalliance.org	●	
Continua Alliance (Health Systems)	http://www.continuaalliance.org	●	●
EPC Global - GS1	www.gs1.org	●	
Hart Communication Foundation	http://it.hartcomm.org/	●	
IPSO Alliance	www.ipso-alliance.org/		●
IERC - European Research Cluster on the Internet of Things	www.internet-of-things-research.eu/	●	●
IIC - L'Industrial Internet Consortium	http://www.iiconsortium.org/		●
IGF - Internet Governance Forum	www.intgovforum.org		●
ISA - International Society of Automation	www.isa.org	●	
LoRa Alliance	www.lora-alliance.org/	●	
MAPI Foundation	www.mapi.net	●	
OASIS Advanced Open Standard for Information Society	www.oasis-open.org		●

Tabella 3 Non-Official Standard Organization: Contributi alla standardizzazione

Non-Official Standard Organization	Web Site	Standard	
		Device - Network Layer	Service - Application Layer
OTA - Online Trust Alliance	https://otalliance.org		●
Open Connectivity Foundation	http://openconnectivity.org/	●	
Open Geospatial Consortium	www.opengeospatial.org	●	
Open Management Group	www.omg.org		●
Open Mobile Alliance	http://openmobilealliance.org	●	●
OWASP - Open Web Application Security Project	www.owasp.org		●
SGIP - Smart Grid Interoperability Panel	http://sgip.org	●	
Software Improvement Group (SIG)	www.sig.eu		●
3GPP	www.3gpp.org	●	
Thread Group	http://threadgroup.org	●	
WAC Wholesale Application Community	www.wacapps.net		●
Wi-Fi Alliance	www.wifialliance.org	●	
ZigBee Alliance	www.zigbee.org	●	

4. Architetture di riferimento

Il termine "architettura di riferimento" o "IoT reference model" si riferisce ad un modello concettuale e generalizzato con il quale sono rappresentati macroscopicamente i domini, i componenti funzionali, le relazioni e le interfacce rilevanti per soluzioni IoT.

I maggiori e più compiuti contributi sugli standard architetturali sono da attribuire a 4 diversi enti di standardizzazione: *International Organization for Standardization (ISO) e International Electrotechnical Commission (IEC); European Telecommunication Standard Institute (ETSI); International Telecommunication United Nation ITU –T.*

ISO / IEC - International Organization for Standardization / e International Electrotechnical Commission

Gli enti ISO e IEC hanno costituito un Working Group congiunto denominato ISO/IEC JTC1. Esso ha prodotto diversi standard aventi lo scopo di definire i componenti chiave delle architetture orientate all'Internet of things.

Il gruppo di lavoro ISO/IEC JTC-1 ha diffuso nel 2014 il "**Preliminary Report sull'Internet of Things**"[2] mentre è ancora in redazione l'atteso documento ISO/IEC WD 30141 Internet of Things Reference Architecture (IoT RA), del quale circola comunque una bozza avanzata.

ISO/IEC 30141 identifica e specifica il modello concettuale dell'IoT (CM), il Modello di Riferimento (RM) e l'architettura di riferimento (RA). L'architettura è descritta secondo le consuete viste architetturali: sistemi, comunicazioni, flusso informativo, casi d'uso, …

[2] http://www.iso.org/iso/internet_of_things_report-jtc1.pdf

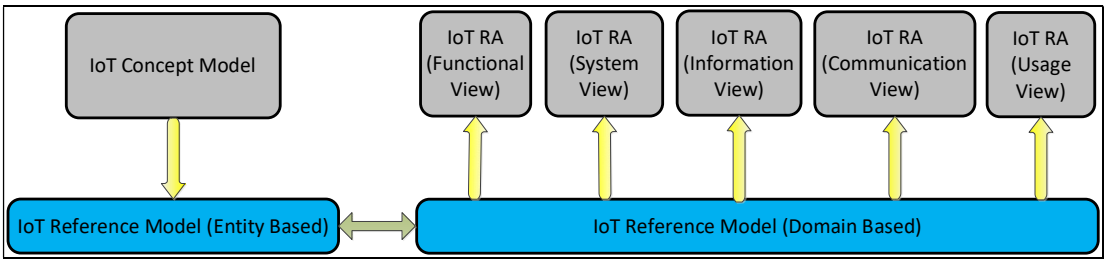


Figura 1 ISO/IEC Reference Model

Tabella 4 - ISO/IEC IoT Standard

JTC 1 Standards
ISO/IEC 29182 Information Technology – Sensor networks – Sensor Network Reference Architecture (SNRA) 2013
Part 1: General overview and requirements
Part 2: Vocabulary and terminology
Part 3: Reference architecture views
Part 4: Entity models
Part 5: Interface Definitions
Part 6: Applications
Part 7: Interoperability Guidelines
ISO/IEC TR 29181 Information technology -- Future Network -- Problem statement and requirements (2012 - 2013)
Part 1 General Aspects
Part 2 Naming and Addressing (currently DTR)
Part 3 Switching and Routing
Part 4 Mobility
Part 5 Security (currently DTR)
Part 6 Media Distribution
Part 7 Service Composition

Tabella 5 ISO/IEC SC29 Media Standard

JTC 1 SC29 – Media Context and control
ISO/IEC 23005-1:2014 Information technology -- Media context and control --
Part 1: Architecture
Part 2: Architecture
Part 3: Sensory Information
Part 4: Virtual World Object characteristics
Part 5: Data formats for interaction devices
Part 6: Common types and tools
Part 7: Conformance and reference software

ETSI - European Telecommunication Standard Institute – OneM2M[3]

ETSI è l'ente di riferimento, insieme con il CEN, per la standardizzazione delle tecnologie ICT nell'ambito della Unione Europea. Su specifico mandato produce le norme tecniche di settore. Produce standard nel campo dell'Information and Communications Technologies includendo: fisso; mobile; radio; la convergenza fra le tecnologie Internet e le radio comunicazioni.

Partecipa a due consorzi dedicati allo sviluppo di standard connessi all'Internet of Things: **OneM2M** partnership e il **Third Generation Partnership Project (3GPP).** Quest'ultima produce standard nel campo delle telecomunicazioni mobili.

Aderiscono ad **OneM2M** le 8 associazioni di standardizzazione nel campo delle telecomunicazioni: ETSI (Europa), TTA (Corea), TTC e ARIB (Giappone) TIA e ATIS (Nord America), CCSA (Cina), TSDSI (India); 5 forum (Broadband Forum, Continua, Home Gateway Initiative (HGI), New Generation M2M Consortium (Japan) Open Mobile Alliance (OMA), partecipano inoltre 200 delle più grandi imprese. L'impegno assunto da oneM2M è la unificazione dei diversi standard delle applicazioni Machine to machine in uso nel mondo nell'ambito sanitario, industriale e della home automation.

ITU – T - International Telecommunication Union (United Nation[4])

ITU ha proposto, già nel 2012, una prima architettura di riferimento. Essa è composta di 4 Livelli Funzionali (Devices, Network, Service & Application Support, Applications) e due Aree Funzionali Comuni: la Gestione e la Sicurezza.

Le norme di riferimento sull'Internet of things sono classificate nella Series Y: Global Information Infrastructure, Internet Protocol Aspects and Next-Generation Networks -2060.

Tabella 6 Lista degli Standard ITU sulle architetture IoT

[3] http://www.etsi.org/technologies-clusters/technologies/internet-of-things

[4] https://www.itu.int/rec/T-REC-Y.2060-201206-I

ITU - T Reccomandation (Standard)
ITU-T Y.2060 (Overview of the Internet of things – 2012)
ITU-T Y.2069 (Terms and definitions for the Internet of things – 2012)
ITU-T Y.2061 (Requirements for the support of machine oriented communication applications in the next generation network environment –2012)
ITU-T Y.2080 (Functional architecture for distributed service networking – 2012)
ITU-T Y.2027 (Functional architecture of multi-connection – 2012)
ITU-T Y.2063 (Framework of the web of things – 2012)
ITU-T F.744 (Service description and requirements for ubiquitous sensor network middleware – 2009)
ITU-T F.771 (Service description and requirements for multimedia information access triggered by tag-based identification– 2008)
ITU-T H.621 (Architecture of a system for multimedia information access triggered by tag-based identification – 2008)
ITU-T Y.gw-IoT-arch (Functional architecture of gateway for IoT applications – in sviluppo)
ITU-T Y.IoT-funct-framework (IoT functional framework and capabilities– in sviluppo)
ITU-T Y.2066 Common Requirements of the Internet of Things

4.1. La proposta ITU -T

Nell'ambito del gruppo di lavoro di Confindustria Digitale (Comitato IoT), citato in premessa, era stata adottata quale prima architettura funzionale di riferimento quanto proposto da ITU-T. Essa è rappresentata nella figura 2.

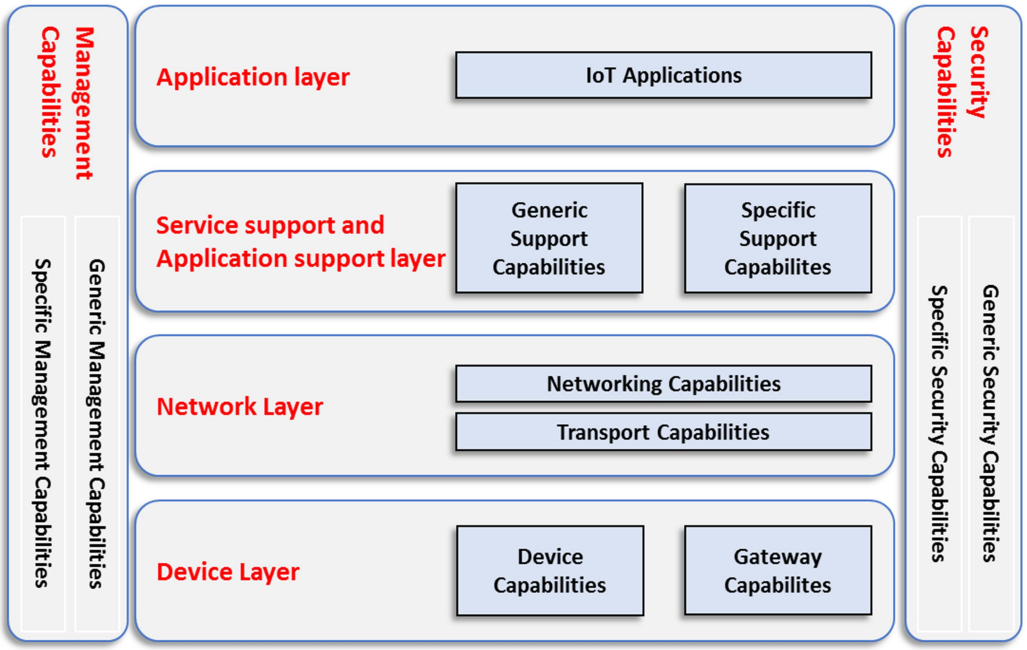


Figura 2: ITU-T IoT Reference Architecture

Tale modello architetturale si compone di 4 livelli (l'application layer, il service support e application support layer, il network layer e il device layer), corredati dalle funzioni di management e di security.

- Device Layer: include tutti quei dispositivi (device) fisici e gateways che possono controllare dispositivi multipli. Questi rappresentano gli "oggetti" (things) dell'IoT e includono una vasta gamma di dispositivi, sensori e attuatori che connessi a Internet inviano e ricevono informazioni. Questo layer può essere logicamente suddiviso secondo due tipi di funzionalità.

    - "Device capabilities"
        - Interazione diretta con la rete di comunicazione: dispositivi sono in grado di raccogliere e caricare le informazioni direttamente (cioè senza l'utilizzo di funzionalità di gateway) verso la rete di comunicazione e possono ricevere direttamente informazioni (ad esempio, i comandi) dalla rete di comunicazione.
        - Interazione indiretta con la rete di comunicazione: i dispositivi sono in grado di raccogliere e caricare le informazioni verso la rete di comunicazione indirettamente solo attraverso le funzionalità di gateway. D'altro lato, i dispositivi possono indirettamente ricevere informazioni (ad esempio comandi) dalla rete di comunicazione.

- "Gateway capabilities"
  - Supporto di interfacce multiple: i gateway sono connessi ai dispositivi attraverso differenti tecnologie come Controller Area Network (CAN) Bus, ZigBee, Bluetooth o Wi Fi. A livello di rete sovrastante, il gateway può comunicare attraverso diverse tecnologie, come ad esempio la rete telefonica pubblica commutata (PSTN), di seconda generazione o terza generazione di reti (2G o 3G), reti LTE, o DSL o tramite LPWA.
  - Conversione di protocolli: quando il gateway connette dispositivi aventi diversi protocolli (es. ZigBee, Bluetooth) o quando il gateway connette da un lato dispositivo con protocolli WSN e dall'altro con protocolli di telecomunicazione.

- Network Layer, la principale funzione di questo livello è quella di garantire la trasmissione affidabile delle informazioni. Include la trasmissione tra i dispositivi attraverso la rete mediante due tipi di funzionalità:

  - Le funzionalità di rete (Network capabilities): forniscono funzioni di controllo competenti di connettività di rete, come accesso e controllo delle risorse di trasporto, funzioni di gestione della mobilità o di autenticazione, autorizzazione e accounting
  - Funzionalità di trasporto (Transport capabilities): per garantire la connettività e il trasporto dei dati dei servizi e delle applicazioni IoT, nonchè il trasporto delle informazioni per il controllo e la gestione

- Service support and application support layer, il "Service support and application support layer" consiste delle "Generic support capabilities" che sono quelle funzionalità comuni che possono essere usate da diverse applicazioni IoT, come il "data processing" o il "data storage". Queste funzionalità possono essere invocate dalle "specific support capabilities". Queste ultime sono invece funzionalità specifiche dedicate all'indirizzamento dei requisiti delle diverse applicazioni.

- Application layer, contiene le applicazioni di gestione dei dati IoT.

- Management capabilities, l'IoT management capabilities include funzioni tipo fault management, configuration management, accounting, performance management e

security management, gestione del ciclo di vita (life cycle management), rating, billing, reporting, etc.

- Security capabilities, questo layer riguarda tutte quelle funzioni necessarie per garantire la sicurezza e la protezione del sistema da minacce esterne. Include almeno le funzionalità necessarie per garantire:
    - A livello applicativo: l'autorizzazione, l'autenticazione, la confidenzialità e l'integrità dei dati, la protezione della privacy, l'anti-virus;
    - A livello di network layer: l'autorizzazione, l'autenticazione, la confidenzialità e l'integrità dei dati sia di segnalazione sia di traffico;
    - A livello di device layer: l'autorizzazione, l'autenticazione, la validazione dell'integrità del device;
    - Specifiche funzionalità per requisiti specifici per applicazioni tipo mobile payment.

4.2. I protocolli per le architetture IoT

In una archiettura informatica la cooperazione tra entità appartenenti allo stesso livello, ma collocate su sistemi diversi, sono realizzate da un insieme di protocolli (protocol); così come tra due entità del medesimo sistema poste su livelli diversi. Nell'ambito dell'IoT la formulazione dei protocolli che meglio si adattano ai requisiti e alle specifiche dei servizi che si intendono realizzare è fonte di una straordinario lavoro di elaborazione e di standardizzazione.

Nel presente documento sono accennati i ruoli e le funzionalità dei protocolli più significativi (per diffusione e aree d'utilizzo). Nella figura sono elencati i protocolli e i relativi layer architetturali di appartenza per gli strati dell'internetworking, con l'avvertenza che alcuni di essi offrono funzionalità su più livelli.

Tabella 7 Protocolli dell'internetworking

Session - communication	**AMQP, XMPP, MQTT, SMQTT, CoRE, DDS, CoAP**
Network Protocol	**IPv4, IPv6, 6LowPan , RPL**
Network Routing Protocol	**RPL, CORPL, CARP**
Data Link Protocol	**Ethernet 802.3, Wifi 802.11a/b/g/n/ac/ah, Bluetooth, BLE, Zigbee 802.14, Dash 7, Rfid, GSM, LTE, LoRaWAN, SigFox, Thread, Weightless**
Connectivity (Physical)	**RJ45, PLC, RS 232, RS 485, Modbus, USB, SPI, ODB2 , Wireless**
Device	**You and Your things**

5. Device Layer

I temi della centralizzazione dei dati provenienti dai dispositivi ai fini della loro elaborazione è un tema tipico dei sistemi industriali. Oggi sono ancor più enfatizzati dal diffondersi delle applicazioni del Cloud Computing.

E' infatti facilmente intuibile come la messa a fattor comune di un'intelligenza centralizzata possa garantire la massima efficienza e flessibilità nella raccolta ed elaborazione di dati da un insieme potenzialmente vastissimo di sorgenti distribuite. L'IoT aggiunge infatti una nuova dimensione al tema dei Big Data: non si tratta solo di un elevato volume di dati, ma soprattutto di un numero massicciamente distribuito di sorgenti dei dati.

Tuttavia le logiche della centralizzazione possono essere in contrasto con i requisiti di servizio di alcuni specifici ambiti applicativi:

- Applicazioni che richiedono bassa latenza (es.: sistemi di gestione del traffico e dei semafori, etc.);

- Applicazioni geo-distribuite (es.: monitoraggio di gasdotti, reti di sensori per monitorare l'ambiente, etc.);
- Applicazioni "fast mobile" (es. smart car, connected railways, etc.);
- Sistemi di controllo distribuiti su larga scala (es.: Smart Grid).

Agendo a livello periferico si possono gestire vaste quantità di dati senza necessariamente passare ogni volta dal centro, con due ulteriori innegabili vantaggi:

- Da una parte, si riduce la richiesta di banda necessaria per raggiungere il Centro;
- Dall'altra si può ipotizzare un aumento nel livello di sicurezza, in quanto le infrastrutture possono rivelarsi maggiormente controllabili o, al peggio, parziamente aggredibili.

Son ambiti dove servono risorse di calcolo e storage locali, in modo tale da fare elaborazioni rapidissime e restituire l'azione nei tempi giusti, il che dà effettivo valore e significato all'applicazione. Da ciò consegue che è necessario spostare in periferia parte dell'intelligenza centralizzata. Per questo l'AIOTI propone la definizione di uno strato specifico nella architettura IoT: "l'Edge Computing".

5.1. Le classi di device

Gli oggetti dell'IoT sono ***Constrained Device***: ovvero dispositivi con restrizioni sulle risorse disponibili e con vincoli dati dalla tipologia di rete e di servizio a cui sono allacciati.

- Vincoli sulla complessità del codice derivante dallo spazio di memorizzazione disponibile (ROM / Flash) ;
- Vincoli sulle dimensioni di stato e buffer (RAM);
- Vincoli sulla potenza di elaborazione (Cicli di clock di CPU al secondo);
- Vincoli sulla potenza disponibile (Corrente assorbita nel tempo);
- Vincoli sull'interfaccia utente e sul deployment di applicazioni (es. la possibilità di impostare le chiavi, eseguire aggiornamento software, etc).

Come suggerito dall'Internet Engineering Task Force – IETF attraverso gli standard RFC 7547 (Management of Networks with Constrained Devices) e RFC 7228 (Terminology for Constrained-Node Networks) I singoli devices sono suddivisibili per classi di appartenenza: capacità di memoria ed elaborazione; energia disponibile; strategia di utilizzo delle comunicazioni wireless.

a) Classificazione per capacità di memoria ed elaborazione

Per poter meglio distinguere fra le differenti tipologie di dispositivi si dovrebbe partire da una loro classificazione basata sulle rispettive *capability* che sono riconducibili alle componenti impiegate ovvero in primis ai componenti elettronici, ai microcontrollori, le interfacce di comunicazione e le tipologie di memoria che sono attualmente disponibili in commercio. Tale approccio conduce quindi alla rappresentazione di tre principali classi di device:

Tabella 8 – Classi di Constrained Devices

Classe	Dim. dati (es.:RAM)	Dim. Codice (es.: Flash)
Classe 0, C0	<< 10 Kb	<< 100 Kb
Classe 1, C1	~ 10 Kb	~ 100 Kb
Classe 2, C2	~ 50 Kb	~ 250 Kb

I dispositivi di Classe 0 (che hanno un basso grado di complessità e sono in forte in analogia con i più semplici sensori attualmente disponibili. I dispositivi di Classe 0 sono integrabili in internet mediante gateway.

I dispositivi di Classe 1 hanno capacità computazionali limitate, supportano funzioni minime di sicurezza, adottano semplici protocolli applicativi. Dispongono di protocolli specifici per l'IoT (come ad esempio il Constrained Application Protocol su UDP [CoAP]) e riescono quindi ad essere connessi alla rete anche senza l'intermediazione di un nodo gateway.

I dispositivi di Classe 2 sono meno vincolati in termini di risorse disponibili e fondamentalmente sono in grado di supportare la maggior parte dei protocolli di rete.

Nelle applicazioni richiedenti basso consumo energetico e con limitatezza di banda sono preferibili protocolli leggeri (MQTT, CoAP, etc).

b) Classificazione in base alla potenza disponibile

I dispositivi differiscono non solo nelle loro capacità di calcolo, ma anche per la potenza e/o energia disponibile. La potenza e/o l'energia disponibile per un dispositivo possono differire notevolmente, da kilowatt a micro-watt, e considerando la cosa in termini energetici si puo' arrivare fino a poche centinaia di micro-joule. Invece di definire classi o gruppi energetici si utilizza il Sistema internazionale come riferimento (unità SI), per indicare un valore approssimativo per una o entrambe le quantità elencate nella tabella seguente.

Tabella 9 - quantità rilevanti di potenza ed energia

Nome	Definizione	Grandezza fisica (SI)
Ps	Potenza media disponibile per il dispositivo all'interno della finestra temporale di funzionamento	W (watt)
Et	Energia elettrica totale disponibile prima che la sorgente di energia si esaurisca	J (Joule)

Ad esempio, in base alla misura potenza Ps ed all'energia Et alcuni dispositivi possono attivare delle funzioni di sleep a basso livello ed entrare in una modalità detta a "basso consumo" prima che l'energia disponibile (in un periodo predefinito di tempo) si esaurisca o addirittura si attivino affinché possano valutare più volte di entrare in questa modalità nel tempo fino all'esaurimento.

Le classi dei dispositivi sono suddivise in base al principio del periodo di richiesta dell'energia (evento, periodicità di utilizzo, ciclo di vita)

Tabella 10 -Classi di limitazione di Energia

Codice	Tipo di limitazione di energia	Esempio di sorgente di potenza
E0	Energia richiesta su base evento	Recupero basato su evento
E1	Energia richiesta su base periodica	Batteria che viene periodicamente ricaricata o sostituita
E2	Energia limitata al tempo di vita	Batteria primaria non sostituibile
E9	Nessuna limitazione diretta di energia disponibile	Alimentazione di rete

Si noti inoltre che alcuni dispositivi E1 possono essere classificati come E2 quando la batteria ricaricabile abbia un numero limitato di cicli di ricarica e non sia ulteriormente sostituibile.

c) Classificazione rispetto alle strategie di utilizzo della potenza nelle comunicazioni wireless

Spesso i *Constrained device* operano in condizioni di trasmissione su rete wireless per cui è determinante valutare l'energy budget ed il duty cycle delle comunicazioni che intraprendono con gli omologhi transceiver.

In presenza di trasmissioni senza fili, la componente radio dei *Constrained device* consuma una parte non trascurabile dell'energia totale consumata dal dispositivo. I parametri di progetto, come lo spettro disponibile, la banda desiderata e il bit-rate auspicato influenzano molto l'energia consumata durante la trasmissione e la ricezione. La durata di trasmissione e ricezione (compreso il campo potenziale di ricezione su antenna) influenzano il consumo totale di energia.

Per gestire al meglio ciò, possono essere utilizzate diverse strategie di utilizzo di energia in base al tipo di sorgente di energia (ad esempio, la batteria e all'alimentazione di rete) e la frequenza con cui un dispositivo deve comunicare.

Le strategie generali per l'utilizzo di energia possono essere:

- Always On. Questa strategia è la più applicata se non vi è alcun motivo per innescare misure estreme di risparmio energetico. Può essere utile impiegare dell'hardware che

consumi poca energia (per limitare il numero di trasmissioni wireless, velocità della CPU, e altri aspetti generali utili al risparmio energetico e necessità di raffreddamento) per cui il dispositivo può essere collegato alla rete per tutto il tempo.

- Normally-Off: Il dispositivo è in fase "dormiente" per lunghi periodi di tempo e una volta che si risveglia si riconnette alla rete. Se l'attivazione della comunicazione avviene di rado, l'aumento relativo di consumo energetico durante la riconnessione può essere considerato accettabile.
- Low power. E' applicabile ai dispositivi che devono operare con piccola quantità di potenza, ma devono essere in grado di comunicare in modo relativamente frequente. Ciò implica che devono essere utilizzati per l'hardware soluzioni a bassa potenza e meccanismi di collegamento specifici (basati su Data Link Layer) e così via. Tipicamente, data la piccola quantità di tempo fra una trasmissione e l'altra, nonostante il loro stato di sleep, questi dispositivi conservano una qualche forma di connessione alla rete. Le tecniche utilizzate per ridurre al minimo il consumo di energia per le comunicazioni di rete includono la minimizzazione dei consumi per la fase di risveglio (wake-up), la regolazione della frequenza delle comunicazioni (tra cui "duty cycle", in cui i componenti vengono accesi e spenti in un ciclo regolare) e la conseguente ottimizzazione degli altri parametri di lavoro.

Tabella 11 Classificazione in base alla connessione

Codice	Strategia	Connessione
P0	Normally off	Riconnesso quando richiesto
P1	Low Power	Appare connesso, ma ha elevata latenza
P9	Always on	Sempre connesso

6. Network Layer

La scelta della connettività necessaria è la base per l'IoT e il tipo di accesso richiesto dipende dalla natura dell'applicazione. Molti dispositivi IoT possono essere serviti da tecnologie radio che operano su spettro senza licenza e che sono stati progettati per garantire accesso a corto raggio, QoS limitate e bassi requisiti di sicurezza. Altre reti richiedono dispositivi e connettività ad alta affidabilità e performance.

Le reti di accesso devono tener conto della diversità dei requisiti che la molteplicità delle applicazioni IoT richiedono. Una semplificazione possibile del mercato dell'IoT è la suddivisione delle applicazioni in "Massive IoT" e "Critical IoT", note anche come "Massive MTC" e "Critical MTC" (Massive Type Communication)

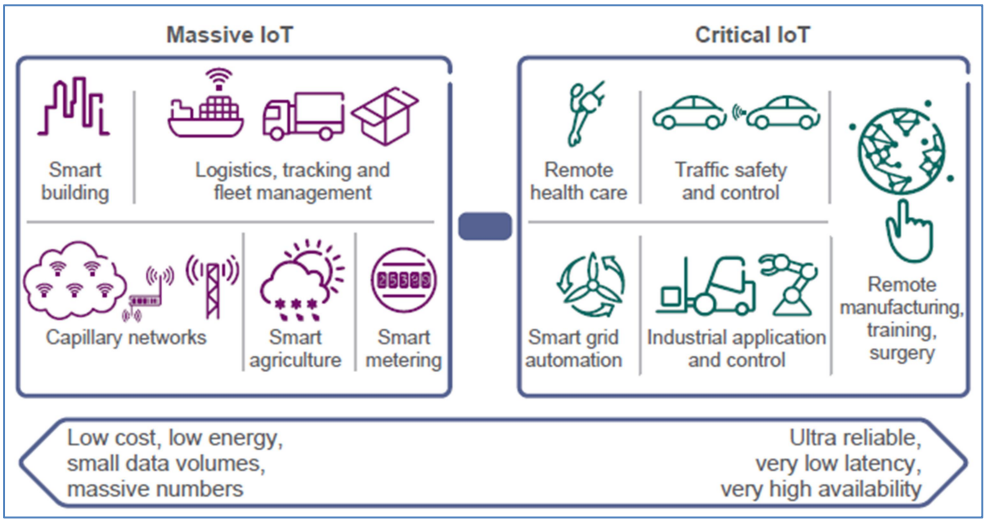


Figura 3 Massive & Critical IoT[5]

- *Massive IoT*: le applicazioni sono caratterizzate da basso costo, basso consumo, e bassa capacità di comunicazione, nonché da un grande numero di dispositivi connessi; *trasporti e logistica, ambiente, casa intelligente, città intelligente, agricoltura, ecc.*

- *Mission Critical IoT*: le applicazioni sono caratterizzate da alta affidabilità, bassa latenza e alta capacità; *automotive, energia (smart grid), sanità, sicurezza, realtà aumentata, automazione della fabbrica, ecc.*

[5] Ericsson White Paper (2016) Cellular Networks for Massive IoT

Requisiti chiave per il segmento "Massive MTC" sono il basso costo dei dispositivi, la lunga durata delle batterie, la copertura radio, la scalabilità.

Nei paragrafi che seguono sono descritti i protocolli di comunicazione in uso attualmente per le WSN e/o in fase di aggiornamento per divenire la base dell'Internet of Things.

Come si è visto nella analisi dei processi di standardizzazione, molti protocolli sono stati sviluppati proponendo specifici e autonomi approcci per la creazione del network, mediante la definizione di protocolli di trasporto proprietari e del conseguente application layer.

Tra le tecnologie che sono applicate solo al livello più basso dello stack OSI sono da segnalare le tecnologie USB e MBUS.

Wireless MBUS *è un protocollo standard europeo sviluppato per applicazioni di metering (M sta per metering). La banda di frequenza utilizzata è quella che va dai 169,400 ai 169,475 MH. Il motivo trainante per la scelta del protocollo W-MBUS a 169 MHz è stato principalmente la bassa frequenza di lavoro, che dovrebbe permettere di raggiungere distanze maggiori e risentire meno dell'attenuazione di eventuali ostacoli. I sistemi a frequenza 169 Mhz permettono una penetrazione degli ostacoli solidi, quali pareti in cemento armato, per questo motivo sono indicati per applicazioni in house, pozzetti interrati, cavidotti, sono indicati per collocazioni verso concentratori fissi*

I protocolli della serie 802.15.x e in generali i protocolli appartenenti all'area delle Wireless Area Networking (WPAN) definiscono propri layers di network, trasporto. Ciò è descritto nei paragrafi relativi agli standard Zigbee e Bluetooth.

Ci sono tecnologie e standard che si basano essenzialmente sui protocolli di base dei servizi Internet IP/ TCP-UDP, quali ad esempio le tecnologie WiFi. Appartengono a questa categoria anche le tecnologie adottate nella building automation, che utilizzando ampiamente la connessione via cavo ethernet adottano l'incapsulamento dei pacchetti secondo il protocollo IP, quali ad esempio gli standard Konnex e LonWorks. Le stesso tecnologie adottano propri devices (gateway) per la connessione alla rete.

6.1. Wireless Connectivity Capability

Per la estensione della rete si fa comunemente riferimento agli acronimi: BAN, PAN, LAN, WAN e LPWAN[6]

Per una analisi più puntuale delle connettività standard di riferimento nel dominio del devices e network layer ci si riferisce:

- Alla tipologia della connettività wireless;
- Ai protocolli di comunicazione;
- Agli intervalli della connettività: intesi come matching tra frequenza operativa / throughput / estensione copertura geografica.

Nella figura è proposta una visione congiunta degli ambiti di applicazione delle reti, impostati rispetto tre parametri:

- la frequenza centrale di riferimento (MHz);
- il data throughput indicato dalla letteratura (kbps);
- il range operativo di massima (distanza di invio / ricezione del segnale in metri).

Per rappresentare uniformemente grandezze fisiche con magnitudo assai diversa, le scale degli assi sono espresse in logaritmi naturale della misura **Ln** (grandezza)**.** Sugli assi sono invece riportati, per immediatezza di comprensione, i valori assoluti corrispondenti.

[6] BAN (Body Area Network); PAN (Personal Area Network); LAN (Local Area Network); WAN (Wide Area Network): LPWAN (Low Power Wide Area Network).

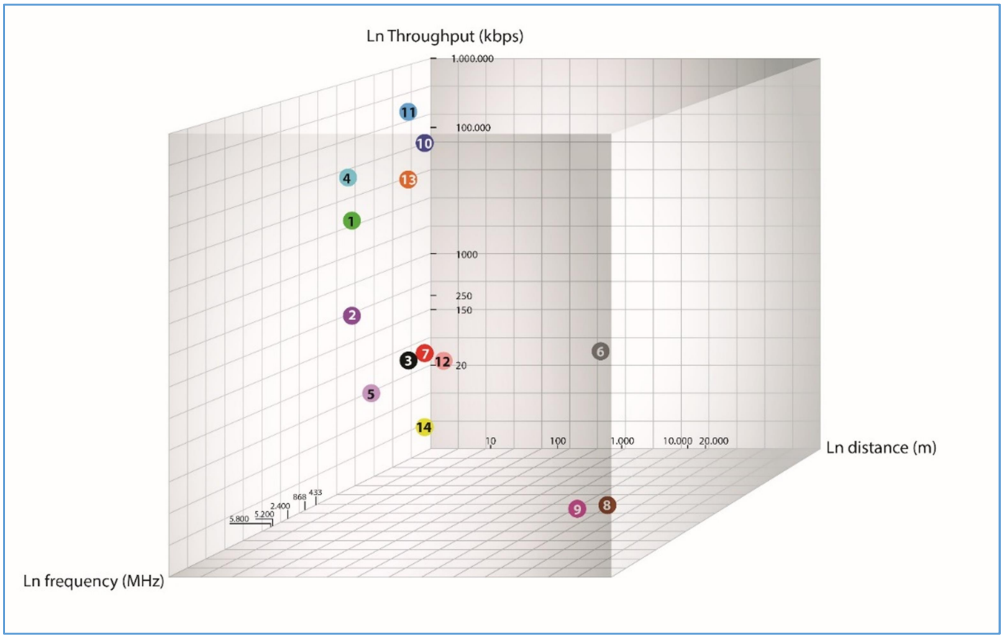


Figura 4 - Wireless Connectivity Capability Cube[7]

N°	Denominazione	Standard o Prodotto	N°	Denominazione	Standard o Prodotto
1	Bluetooth v4 Low Energy	*Bluetooth SIG*	8	LoraWan	*LoraWan - Ultra Narrow Band*
2	Bluetooth Core	*Bluetooth SIG (802.15.1)*	9	SigFox	*Cooperative - Ultra Narrow Band*
3	Cooperative-ITS	*DSRC*	10	Wi-Fi	*IEEE 801.11n*
4	DS -UWB	*UWB*	11	Wi-Fi	*IEEE 801.11ac*
5	IETF 6Low PAN - IEEE 802.15.4	*IETF 6Low PAN*	12	Wi-Fi	*IEEE 801.11ah*
6	NB-IoT	*NB - IoT 3GPP*	13	Wireless Industrial	*Wireless Industrial*
7	Thread	*IEEE 802.15.4*	14	Zigbee Smart Energy	*IEEE 802.15.4*

Tabella 12 - Legenda Capability Cube

Per le applicazioni IoT a basso consumo che necessitano di una copertura ad ampio raggio (Low Power Wide Area Coverage, LPWA), ci sono attualmente due possibili tecnologie di accesso alternative:

- Le tecnologie LPWA licenziate;
- Le tecnologie LPWA non licenziate.

Il segmento "Critical MTC" indirizza ad esempio le applicazioni di controllo e sicurezza del traffico, controllo e connettività wireless per i processi industriali e le applicazioni Sanitarie, Tali applicazioni richedono alta affidabilità e disponibilità della connessione di rete, bassa

[7] Exprivia (2017) XIX AISEM Conference Proceeding

latenza, tempi di trasmissione molto brevi e possibilità di dare accesso immediato ai servizi di priorità più alta. Questo segmento è proprio delle tecnologie Wireless Hart, 802.11.ac, 5G.

6.2. Connettività Short Range

Nel segmento dell'accesso "short range" si sviluppano le capillary networks. Reti che usano tecnologie di accesso radio "short-range" per fornire la connettività a gruppi di dispositivi.

Esempi di tecnologie radio usate dai dispositivi e dai sensori delle capillary network sono Zigbee, Thread, Bluetooth, Wifi IEEE 802.11ah.

Tabella 13 Layer coperti dai protocolli Wifi - Bluetooth, Zigbee e Thread

Application				
Network / Transport	TCP / UDP / IP			
Physical / link	IEEE 802.11		IEEE 802.15.4	IEEE 802.15.4

La connessione delle reti capillary alla infrastruttura globale di comunicazione può essere effettuata attraverso una rete radiomobile (soluzione wide area network o cellulare indoor), una rete satellitare o una cooperazione tra le due. Un gateway tra la rete cellulare/satellitare e la capillary network agisce da aggregatore. Anche in questo caso la tecnologia cellulare/satellitare fornisce benefici se utilizzata come opzione di bridging, vale a dire come una soluzione di aggregazione e routing, attraverso l'uso di gateway. In tal caso la combinazione di accesso mobile licenziato e non licenziato consente il riutilizzo di funzioni della rete licenziata per quanto concerne la sicurezza, la gestione dei dispositivi, la fatturazione e la QoS, senza la necessità che ogni dispositivo connesso al gateway sia un dispositivo con subscription.

6.2.1. *Zigbee*

Zigbee[8] è il nome dato a uno specifico insieme di protocolli basati sullo standard IEEE 802.15.4 dedicato alla wireless personal area networks (WPAN). La relazione esistente fra ZigBee Alliance e IEEE 802.15.4-2003 è simile a quella esistente tra IEEE 802.11 e la Wi-Fi Alliance.

Il protocollo sviluppato dalla ZigBee Alliance ha lo scopo di supportare reti di oggetti a costi e consumi energetici minori rispetto ad altri più noti protocolli wireless. Caratterizzato da una velocità di trasferimento dei dati relativamente bassa (250 Kbyte/s a 2.4 Ghz,), ha però interessanti caratteristiche di sicurezza e la possibilità di collegare tra loro un alto numero di unità, cosa che lo rende particolarmente adatto a funzionalità di controllo, come nel campo della Domotica. E' stato infatti concepito per essere integrato negli oggetti di uso comune. Si tratta inoltre di uno standard aperto, cosa che dovrebbe garantirne una buona diffusione. Protocolli ZigBee sono progettati per l'uso in applicazioni embedded che richiedano un basso transfer rate e bassi consumi. Non adotta direttamente il protocollo IP, preferendo la soluzione proprietaria Zigbee e definendo proprie API per le interfacce di comunicazione.

L'entità *Zigbee stack data* provvede al servizio di trasmissione dei dati, cosi come l'entità *Management* provvede agli altri servizi. Ciascuna entità di servizio dispone di una interfaccia verso il layer superiore attraverso il *Service Access Point* (SAP) e ciascun SAP supporta le primitive dei servizi relativi alle funzionalità richieste. Il protocollo Zigbee, definito dallo standard IEEE 802.15.4-2003 supporta il network layer e il framework dell'application layer che comprende anche le applicazioni di sub layer per la gestione dello Zigbee Device Object (ZDO).

ZigBee Smart Energy v2.0

- Adotta i requisiti di base per la sua applicabilità nell'ambito delle Smart Grid e le specifiche NIST9 per la sua adozione negli Stati Uniti.
- Adotta ZigBee IP stack: 6lowPAN (IPv6) per il formato dei pacchetti e le regole di frammentazione dei pacchetti.

[8] http://www.zigbee.org/what-is-zigbee

[9] https://www.nist.gov/

- Adotta il Protocollo di Routing del Low power and lossy networks (RPL), come definite da IETF ROLL charter
- L'Application layer protocol è in elaborazione da parte del Comitato IETF : CoAP e SOAP su UDP
- Adotta : Embedded Service Location Protocol (IETF),
- Ha una nuova release formato MAC (TG IEEE 802.15.4e),
- Meter Access Side Communications standard (TG IEEE 802.15.4g),
- Il livello Applicazione è definito con lo IEC 61968 CIM. I messaggi sono in formato XML.

6.2.2. *Bluetooth*

La tecnologia Bluetooth[10] opera nella banda di 2.4 GHz, in un range attivo compreso nelle aree sino a 100 m di raggio. La differenza dipende dal tipo di device. Il data rate di picco è pari a 3 Mbps. La tecnologia è omni direzionale, non occorre operare in linea di vista (salvo considerare le limitazioni dovute alla ampiezza di banda).

Gli apparati certificati Bluetooth operano su 3 classi di attività.

Tabella 14 Classi di devices Bluetooth

Classe	Potenza (mW)	Potenza (dBm)	Distanza (m)
1°	100	20	Fino a 100
2°	2,5	4	Fino a 10
3°	1	0	Fino a 1

Secondo le **Core Specification 5.0**[11], emanate dal SIG (Special Interested Group) Bluetooth nel dicembre del 2016, vi sono due tecnologie wireless bluetooth: *Basic Rate (BR) e Low Energy (LE)*. Entrambe adottano soluzioni per il discovery dei devices, per l'ingaggio della connessione e il controllo dela connettività. BR include soluzioni opzionali avanzate: Enhanced Data Rate (EDR), Alternate Media Access Control (MAC) ed estensione del layer fisico (PHY). BR offre connessioni sincrone ed asincrone con data rate compreso tra i 721. Kbps e 2.1 Mbps, con

[10] https://www.bluetooth.com/
[11] https://www.bluetooth.com/specifications/adopted-specifications

velocità sino a 52 Mbps per connessioni 802.11 (WiFi). LE è progettato per soluzioni con bassa data rate e necessità di bassi consumi.

I devices di ultima generazione possono implementare entrambe le configurazioni permettendo di variare la consistenza e la topologia delle reti, nonché la qualità del servizio.

6.2.3. *Thread*

Lo stack Thread[12] è uno standard aperto, per la comunicazione low power wireless tra device. Basato sullo standard 6LowPan è stato progettato specificamente per le applicazioni dell'Home Automation, le sue caratteristiche:

- Semplice installazione del network, grazie a funzioni di autoconfigurazione della rete tra nodi Thread;
- Un nodo è abilitato alla connessione solo con comunicazioni criptate;
- Sufficientemente flessibile per comprendere tutti i bisogni di connessione dei dispositivi della domotica;
- La tecnologie mesh e spread spectrum permettono di costruire topologie variabili e ridurre le possibili interferenze;
- Funziona anche in presenza di più punti non attivi o guasti.

[12] http://threadgroup.org/

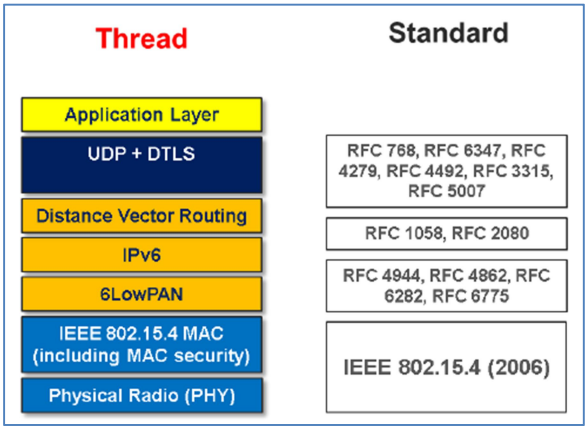


Figura 5 Stack Thread[13]

6.2.4. *Industrial Wireless*

La normativa per le reti di comunicazione per l'automazione industriale è definita in ambito internazionale dal sottocomitato 65C "Industrial networks" *dell'International Electrotechnical Commission*[14] (IEC). L'aspetto caratterizzante dell'Industrial Wireless non è il numero di elementi trasmissivi impiegati, com'è per il mercato Consumer e per le reti dell'Information Technology, ma il considerare l'impiego di ciascun elemento trasmissivo nei vari decenni di vita di un impianto industriale, la riduzione delle interferenze e la relativa latenza della comunicazione (spesso in real time).

A livello europeo, l'attività di standardizzazione è svolta dal comitato tecnico 65X del CENELEC (www.cenelec.eu) che collabora strettamente con il comitato tecnico IEC 65 in modo che la normativa che sarà stabilita a livello internazionale sia in linea con le regole e gli interessi europei. A livello nazionale l'attività è svolta dal sottocomitato tecnico 65C del Comitato Elettrotecnico Italiano (www. ceiweb.it).

Con essa sono stabiliti sia i requisiti generali per le reti di comunicazione via filo e wireless, sia le specifiche norme delle reti per l'automazione e il controllo dei processi produttivi. Particolare attenzione è posta nella definizione di regole di gestione dei sistemi di comunicazione wireless che permettano che i vari sistemi di comunicazione installati in uno stesso impianto industriale possano coesistere.

[13] Thread Group (2015) Thread Stack Fundamental
[14] www.iec.ch

Industrial Wireless
IEC/TS 62657 - Part 1 Industrial communication networks - Wireless communication Requirements and spectrum considerations - 2013
IEC/TS 62657 - Part 2 Industrial communication networks - Wireless communication networks Coexistence management - 2014 draft

Tabella 15 - Industrial Wireless Standard

Tra gli aspetti chiariti nel primo documento, vi sono i motivi per cui lo spettro di frequenza per le applicazioni di automazione industriale deve stare tra un minimo di 1,4 GHz e un massimo di 6 GHz.

Una specifica applicazione dell'Industrial Wireless è data dal Protocollo WirelessHART. Ad esso corrisponde una tecnologie di sensor networking basata sull' "*Highway Addressable Remote Transducer Protocol* (HART)". Sviluppato da un consorzio di imprese (ora Fondazione HART). Lo standard propone gli strumenti hardware e software per il rapido dispiegamento di una rete wireless in ambito industriale operando nella banda ISM a 2.4 GHz.

WirelessHART
IEC 62591: 2010 Industrial communication networks - Wireless communication network and communication profiles - WirelessHART™
IEEE 802.15.4™-2011 - IEEE Standard for Local and metropolitan area networks--Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs)

Tabella 16 - WirelessHART Standard

6.3. Connettività Long Range

Le esigenze del mercato IoT, con particolare riferimento al "Massive IoT", possono essereno in un certo senso divergenti rispetto a quelle degli utenti che utilizzano i servizi di telefonia mobile. Nel caso dell'IoT è spesso sufficiente una bassa velocità di trasmissione con conseguente limitato consumo di banda, mentre parametri importanti sono il costo contenuto del terminale radio e il fatto che si abbia un ridottissimo consumo energetico, tale da garantire un funzionamento di svariati anni con alimentazione a batteria. Le applicazioni IoT possono

richiedere infrastrutture di rete wireless con celle in grado di gestire un numero potenzialmente elevato di oggetti e con una copertura più estesa rispetto al servizio voce o dati.

Da qui la nascita di una nuova categoria di reti mobili, le reti Low-Power Wide-Area (LPWA).

Le reti LPWA sono progettate per rispondere alle quattro caratteristiche (riassunte in inglese sotto quattro "L"), che costituiscono i punti critici dell'Internet delle Cose:

- Low Power = Basso consumo energetico
- Long Range = Lungo raggio e buona penetrazione degli ostacoli solidi
- Low Traffic = Basso traffico
- Low Cost = Basso costo

La facilità di configurazione e gestione, l'eccezionale penetrazione sul territorio, con celle di raggio pari o superiore ai 40 Km, la flessibilità e adattabilità, la bidirezionalità, la sicurezza, il basso consumo (durata delle batterie dei sensori che arriva a oltre 10 anni) e, soprattutto, il basso costo, rendono le reti LPWA risorse preziose per la copertura di aree attualmente irraggiungibili, come quelle agricole e rurali.

Si tratta di reti particolarmente adatte alla gestione dell'IoT, in quanto il loro scopo è raccogliere dati da un alto numero di sensori, localizzati su superfici vaste e spesso di difficile accessibilità, dove sarebbe anti-economico arrivare con una delle reti Long Range tradizionali, soprattutto dal punto di vista energetico (si pensi al consumo e alla relativa durata della batteria di sensori connessi con SIM 3G/4G tradizionali). L'ovvio limite di una rete LPWA è la quantità di dati trasmissibili nell'unità di tempo, che è estremamente limitata (una rete LPWA risulta pertanto inadatta a trasferire -ad esempio- flussi audio/video).

Le caratteristiche tecniche di una rete LPWA possono quindi essere così riassunte:

- Operatività a basse frequenze (tipicamente sotto 1 GHz);
- Estrema efficienza energetica (es.: batterie per la trasmissione dei sensori di durata anche superiore ai 10 anni);

- Utilizzo di bande di frequenza licenziate (es.: 900 MHz) o non licenziate (es.: ISM 868 MHz);
- Ampia portata (es.: celle di raggio superiore ai 10 Km);
- Efficiente copertura indoor (l'utilizzo di basse frequenze consente un'elevata qualità del servizio anche sottoterra o dietro muri di cemento armato);
- Robustezza ad interferenze e disturbi;
- Unità ricetrasmittenti estremamente piccole e potenzialmente SIM-less;
- Banda stretta con conseguente limitata quantità di messaggi raccolti da ogni sensore nell'unità di tempo.

6.3.1. *Tecnologie Low-Power Wide-Area (LPWA) licenziate*

Le reti WAN operano tipicamente su spettro di frequenze licenziate e storicamente sono sviluppate per soddisfare i requisiti dei servizi voce e dati di alta qualità. Per l'IoT, in particolare per il Massive IoT, i requisiti sono differenti (basso costo dei dispositivi, lunga durata delle batterie, copertura radio anche in ambienti di difficile raggiungibilità, scalabilità). Le esigenze di copertura cambiano a seconda delle applicazioni: ci sono per esempio casi che richiedono dispositivi stazionari e localizzati all'interno degli edifici e altri che invece necessitano di una copertura geografica globale (come ad esempio il monitoraggio di un container).

L'importanza delle reti LPWA per l'IoT è stata riconosciuta dalla GSM Association[15] (GSMA). L'Associazione che raggruppa gli operatori mobili di recente ha lanciato la "*Mobile IoT Initiative*", sostenuta da 26 tra operatori di telefonia mobile e società OEM produttrici di chipset, moduli e infrastrutture, per guardare alle tecnologie Low Power Wireless Access (LPWA) nel contesto delle bande licenziate. L'associazione si aspetta che le specifiche iniziali

[15] http://www.gsma.com/

per le soluzioni LPWA sono comprese nella Release 13 del 3GPP[16], mentre le prime soluzioni commerciali complete sono arrivate nel corso dell'anno 2016.

Sono state proposti sia la evoluzione delle tecnologie pre esistenti (EC – GSME e LTE) sia la introduzione di una nuova tecnologia LTE Cat-M2 o NB-IOT.

EC-GSM -IoT

La tecnologia GSM è ancora la tecnologia dominante in molti mercati e la maggior parte delle applicazioni M2M oggi usa accesso e connettività GPRS/EDGE.

Il GSM continuerà ancora ad avere un ruolo nell'IoT grazie alla copertura globale che oggi garantisce, al time to market e ai costi ridotti. Detto ciò, la 3GPP Release 13 migliora ulteriormente GSM: la funzionalità EC-GSM, infatti, garantisce una migliore copertura fino a 20dB rispetto al GPRS sulla banda a 900MHz.

Tale ampliamento della copertura viene ottenuto mediante nuove codifiche di canale e la ripetizione dei messaggi per aumentarne la probabilità di ricezione. Lo standard EC-GSM rimane compatibile con il GSM e consente di aggiungere le funzionalità IoT mediante un upgrade software sulle reti di accesso radio GSM di recente costruzione, sfruttandone quindi la copertura globale.

Tecnologie LTE

La tecnologia Long Term Evolution (LTE) è quella che domina oggi il Mobile Broadband, la sua diffusione/copertura si sta espandendo rapidamente.

Per venire incontro alle nuove esigenze di connettività del segmento del Massive IoT il 3GPP Release 13 comprende anche novità per il segmento LTE sia per le reti di accesso sia per i dispositivi IoT. Lo scopo dei nuovi standard è:

- Ridurre i costi dei dispositivi diminuendo i costi dei moduli LTE, operando sulla banda e la modalità di trasmissione, sulla memoria e sulla complessità del dispositivo, per esempio con l'introduzione dei terminali LTE-M (Cat M1) e NB-IoT (Cat M2).
- Aumentare la durata delle batterie attraverso meccanismi di "Power Saving Mode" ovvero l'Extended Discontinuous Reception" (eDRX).

[16] http://www.3gpp.org/release-13

- Aumentare l'area di copertura outdoor e la penetrazione indoor per raggiungere dispositivi IoT: come i contatori (smart meters) posizionati nei piani interrati degli edifici. La copertura aumenta di 15dB con LTE-M e di circa 20dB col Nb-IoT e EC-GSM.
- Garantire il supporto di grandi quantità di dispositivi IoT connessi.

I veri dispositivi per l'IoT a basso consumo e larga copertura (LPWA) sono i cosiddetti CAT-M1 e CAT-M2.

LTE Cat-M1

I dispositivi Cat-M1 introdotti nella release 13 di 3GPP (Marzo 2016) sono i primi a ridurre i consumi, semplificare la complessità (abbattendo i costi) e aumentare la copertura per applicazioni IoT. La banda di canale è di 1,4 MHz, all'interno del canale LTE che può arrivare fino a 20 MHz di larghezza di banda.

La limitata larghezza di banda è uno dei principali fattori che semplificano il modem e quindi ne abbattono i costi, ma altre caratteristiche come le modalità di trasmissione e ricezione discontinue (eDRX), la limitazione della segnalazione e modalità di *power save* consentono di limitare i consumi. Per estendere la copertura rispetto ai dispositivi attuali vengono utilizzati nuovi formati semplificati e protetti di codifica di canale, insieme a moduli di ripetizione dei messaggi per aumentarne la probabilità di ricezione.

LTE Cat-M2 o NB-IOT

In aggiunta ai dispositivi Cat-M1, la release 13 del 3GPP ha introdotto anche il dispositivo Cat-M2 con larghezza di banda limitata a 200 KHz. Il canale a 200 KHz può coesistere all'interno di canali LTE, nelle bande cosiddette di guardia tra un canale LTE e quello adiacente, oppure su una frequenza a parte.

Anche i dispositivi Cat-M2 supportano una copertura estesa, grazie a nuove codifiche di canale e la ripetizione delle trasmissioni.

La tecnologia NB-IoT è una soluzione che coniuga le prerogative di una rete LPWA *Low Power Wide Area,* permettendo di creare un sistema pervasivo ed interconnesso, con quelle delle reti

cellulari – 4G. Il tema della sicurezza è riconosciuto come un tema cruciale per le implementazioni M2M.

La nuova tecnologia offre il supporto a tutti i requisiti delle tecnologie LPWA, ovvero

- Miglioramento della copertura indoor (fino a 20 dB superiore)
- Supporto di un numero elevato di device a basso throughput (fino a 200.000 per ogni cella di 200 KHz)
- Supporto alla lunga durata delle batterie. (Oltre i 10 anni)
- Scalabilità: La soluzione è scalabile aggiungendo più portanti (ovvero celle) di 200kHz di banda

La *Mission Critical Machine Type Communication* è richiesta nei casi di controllo in tempo reale e automazione dei processi dinamici in vari campi, tra i quali l'industria, la distribuzione energetica, i sistemi di trasporto intelligenti, la sanità da remoto.

I requisiti fondamentali del Mission Critical Machine Type Communication sono:

- Alta affidabilità della connessione (Reliability)
- Alta disponibilità della connessione (Availability)
- Latenza end to end molto bassa, dell'ordine di pochi millisecondi.

La latenza è il tempo che intercorre tra la produzione dei dati, ad esempio al sensore, e il loro arrivo al ricevitore. Si veda la figura sottostante. Il requisito più stringente previsto è dell'ordine del millisecondo, . Il requisito sulla interfaccia radio è un ritardo di 100 µs per ciascuna direzione [17]

[17] ITU-T ITU Tecnology Watch Report - Tactile Internet, 2014

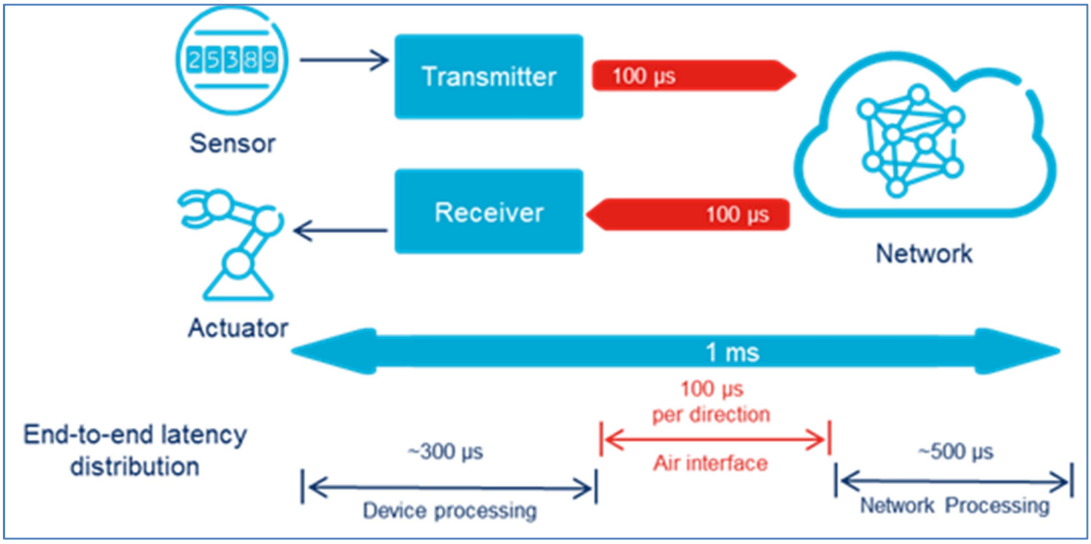


Figura 6: Distribuzione della Latenza

Per affidabilità (reliability) si intende la capacità di garantire la trasmissione dei dati con la latenza richiesta. Il requisito di affidabilità dipende dalle applicazioni. Per l'automazione industriale è dell'ordine di 1 su un miliardo, ovvero si tollera che solo un messaggio su un miliardo possa essere perso o che abbia un ritardo superiore alla latenza richiesta[18].

La disponibilità del sistema richiede che la connessione sia attiva quando richiesto al 99.999% dei casi.

L'opportunità di fornire anche il *Mission Critical Machine Type Communication* con la medesima tecnologia di accesso radio con cui sono servite anche le applicazioni Mobile Broadband, i media e il massive MTC permette ai fornitori di connettività di evitare la frammentazione dello spettro e di sfruttarne al massimo le potenzialità. I fornitori di connettività inoltre offrono in questo modo supporto a nuovi servizi il cui potenziale di business è ancora da sviluppare, senza la necessità di implementare una rete parallela, per la quale sarebbe necessario assegnare nuovo Hardware, nuovo Sotware e nuove risorse spettrali.

La tecnologia prevede tre modalità di funzionamento differenti:

- Stand-alone – in sostituzione di uno o più canali GSM
- Guard band – utilizzando i resource blocks non utilizzati ai margini della portante LTE

[18] ETSI report – TR 102 889-2

- In band – utilizzando resource blocks all'interno di una portante LTE

Grazie all'accordo ottenuto al 3GPP TSG RAN WG1 Meeting #69[19] tutti i maggiori vendor TLC (Nokia, Ericsson, Huawei, Intel, Qualcomm) supporteranno una singola soluzione armonizzata.

A livello radio (RAN1) le modalità di trasmissione in uplink e downlink, prevedono:

- Ampiezza di banda pari a 180 kHz sia per uplink sia per downlink
- Modulazione OFDMA (Orthogonal Frequency-Division Multiple Access) per la trasmissione in downlink con sottoportanti da 15 kHz per tutti gli scenari standalone, guardband, in-band
- Modulazione SC-FDMA (Single-carrier FDMA) multi-tono per la trasmissione in uplink su sottoportanti da 15 kHz e con possibilità di una modalità single-tone su sottoportanti da 3.75 kHz oppure 15 kHz. Sono previsti meccanismi per la riduzione del PAPR (Peak-to-Average Power Ratio) per un uso efficiente della batteria
- Allo stesso modo la standardizzazione sta lavorando su segnalazione (RAN2), requisiti RF (RAN4), architettura di sistema (SA2), Sicurezza (SA3).

I miglioramenti sulle reti radiomobili richiesti dal Massive MTC sono già stati standardizzati nel 3GPP. Lo standard è stato approvato nel giugno 2016.

I requisiti del Mission Critical MTC sono considerati anche nello sviluppo tecnologico ed architetturale del 5G.

6.3.2. *Tecnologie Low-Power Wide-Area (LPWA) non licenziate*

Il panorama delle tecnologie LPWA si completa con le alternative non licenziate, ovvero con le soluzioni che rendono l'infrastruttura e il servizio indipendenti da un operatore di telecomunicazioni e soprattutto non sono, per ora, soggette a specifiche tassazioni. Queste tecnologie trovano la loro applicazione naturale negli ambiti "Massive IoT".

L'indirizzo verso questo approccio è guidato, oltre che dall'indipendenza, da alcune caratteristiche importanti, tra cui:

[19] http://www.3gpp.org/DynaReport/TDocExMtg--RP-69--31198.htm

- la disponibilità attuale della tecnologia;
- la semplicità della gestione dello spettro (appunto non licenziato);
- la semplicità tecnica della componente TX/RX del sensore che porta i suoi costi a livelli notevolmente più bassi rispetto a qualsiasi altre tecnologie;
- l'algoritmo per la trasmissione e l'utilizzo del mezzo condiviso in grado di ottimizzare al massimo la durata della batteria, capace di raggiungere i 10 anni di durata a seconda degli scenari;
- i costi inferiori delle base station e quindi dell'infrastruttura di copertura e della sua gestione;
- i costi e i tempi inferiori dell'attivazione del servizio per i singoli sensori, non SIM-based e quindi slegati da processi di SIM-provisioning;
- gli algoritmi di sicurezza normalmente integrati;
- l'apertura della piattaforma ad integrazioni applicative proprie, indipendenti da terzi.

Nell'ambito delle reti LPWA non licenziate stanno prendendo principalmente piede due diverse alternative:

- la tecnologia LoRa® wireless (Long Range), nata dal contributo di aziende unitesi in un'alleanza con l'obiettivo di redigere le specifiche Long Range wireless per applicazioni IoT nelle bande 868 MHz e 915 MHz (larghezza di banda minore di 500KHz);
- i servizi Ultra-NarrowBand, come SigFox, sviluppati con tecnologie proprietarie, caratterizzati da un bit rate minore di 100bps, tipicamente nella banda 868 - 900 MHz (larghezza di banda 100 Hz).

6.3.3. *LoRa®, LoRa® Alliance e LoRaWAN™*

Con il termine LoRa® (Long Range) Alliance ci si riferisce ad un'associazione no-profit aperta di cui fanno parte multi-nazionali delle telecomunicazioni, vendor, system integrator, produttori di sensori, start-up, etc. che si pone l'obiettivo di sviluppare nuovi standard per le reti LWAN

dedicate all'IoT, aventi sensori alimentati da batteria e coperture a lungo raggio. La LoRa® Alliance concentra le sue attività nello sviluppo della soluzione attorno al LoRa® e al LoRaWAN™.

LoRa® è il livello fisico, ovvero la modulazione wireless che caratterizza la tecnologia, LoRaWAN™ descrive i protocolli e l'architettura del sistema e della rete.

Le caratteristiche del LoRa® sono proprie di una modulazione a spettro distribuito (Spread-Spectrum), consentendo una demodulazione di ben 20 dB sotto il livello di rumore, cosa che estende il link budget a 150 o 160 dB a seconda delle frequenze utilizzate. Ne deriva una elevatissima sensibilità di ricezione, collegamenti robusti, forte resistenza alle interferenze, basso consumo in trasmissione. Si tratta della prima versione commerciale di una modulazione utilizzata per decenni in applicazioni militari e spaziali.

A tali risultati, che rendono interessante LoRa®, contribuiscono anche scelte architetturali e di protocollo che LoRaWAN™ definisce. In particolare:

- La tecnologia evita qualsiasi approccio mesh e considera l'architettura "a stella" come modello efficace per evitare sprechi di risorse di rete e di batteria del sensore, non interessato ad inviare informazioni non proprie.
- Il singolo sensore non si registra specificatamente ad una singola base station, ma le sue informazioni sono ricevute contemporaneamente da più gateway. Questi non elaborano il dato e inoltrano le informazioni al network server, la componente di governo centrale dell'architettura, che sgrava la rete da qualsiasi compito di gestione di handover e di sicurezza. Il network server ha l'intelligenza per gestire le informazioni eventualmente ridondate, per decidere in tempo reale il miglior gateway per le comunicazioni verso il sensore e per determinare adattamenti di velocità di trasmissione. Tutto ciò riduce notevolmente la complessità della rete, l'intelligenza dei gateway e quindi il costo delle base station e lo scambio di informazioni di controllo con i sensori.
- I sensori trasmettono solo quando è necessario, ossia quando hanno dati da inoltrare. In questo approccio asincrono mancano tutte quelle trasmissioni di sincronizzazione

tipiche di una rete GSMA, a vantaggio di un'efficienza unica nella gestione della batteria.

- LoraWAN™ permette la possibilità di adattare il rate di trasmissione alle condizioni della rete; questo vuol dire ad esempio che sensori prossimi al gateway possono trasmettere ad un rate più alto limitando il tempo di trasmissione e liberando prima il canale a favore di sensori che necessitano di un rate più basso per condizioni meno favorevoli; tutto ciò, insieme alla possibilità di incrementare le capacità della rete semplicemente aggiugendo base station, rende la tecnologia flessibile e fortemente scalabile in termini di capacità.
- LoraWAN™ permette la classificazione dei sensori in tre differenti classi per adattare il comportamento trasmissivo bidirezionale alla tipologia di applicazione richiesta e sfruttare in maniera efficace la banda condivisa, preservando al massimo le batterie dei sensori:

Tabella 17 Classe di sensore per alimentazione

A - all	Sensore alimentato a Batteria o attuatore senza particolari limiti di latenza di comunicazione. Alta efficienza nel consumo della batteria.
B – beacon	Attuatore alimentato a Batteria, con garanzia di comunicazione attraverso sincronizzazione a beaconing.
C - continuous	Attuatori alimentati a rete che necessitano di comunicazione downlink continua senza soffrire latenza.

- Questo vuol dire poter preservare al massimo la batteria di quei sensori, tipicamente di puro metering (Classe A), che possono ricevere comunicazioni anche solo dopo aver trasmesso; vuol dire poter limitare la latenza di comunicazione dal centro agli attuatori per quei sistemi che devono risparmiare batteria ma che necessitano di comunicazioni regolari dal centro (Classe B); vuol dire poter garantire latenza nulla per quei attuatori, magari alimentati dalla rete e non da batteria che richiedono latenza nulla nella comunicazione dal centro (Classe C)

- LoraWAN™ integra nativamente meccanismi di sicurezza per l'autenticazione e il riconoscimento dei sensori e la garanzia della riservatezza del dato (AES encryption con scambio chiave basato su identificativo IEEE EUI64.

Diversi primari Operatori Europei (es.: Bouyges, Swisscom, Proximus, Orange etc.) stanno cominciando il deployment di soluzioni LoRa® con ampia copertura territoriale. I casi d'uso proposti sono molteplici: ottimizzazione di servizi di manutenzione, gestione dei flussi di traffico, monitoraggio del consumo di energia o di acqua, soluzioni sanitarie di monitoraggio di pazienti a distanza, etc.

6.3.4. *SigFox® - Ultra-NarrowBand*

In ambito LPWA, molti vendor stanno sviluppando soluzioni Ultra-NarrowBand (UNB), sia seguendo lo standard Weightless-N[20], sia sviluppando tecnologie di rete proprietarie.

Il concetto di base è disporre di sistemi di trasmissione wireless operanti sulle frequenze "senza licenza" ISM (Industrial, Scientific and Medical), in grado di coprire notevoli distanze (long-range) grazie alla elevatissima sensibilità del ricevitore che sfrutta la tecnologia Ultra Narrow Band[21]. Anche i consumi energetici sono particolarmente ridotti in quanto il dispositivo remoto va in trasmissione per pochi secondi e per un numero limitato di volte al giorno.

In questo senso un esempio di tecnologia proprietaria è il sistema Sigfox[22] per la connettivitò UNB di oggetti sparsi sul territorio. Le caratteristiche tecniche principali sono:

- potenza di trasmissione di ogni singolo oggetto di 25 mW; questo comporta bassi consumi con durata delle batterie potenzialmente superiori ai 10 anni;
- link budget di 162 db;
- basso throughput (tipicamente 100 bps) dove ogni singolo messaggio consta di 12 bytes in uplink e 8 bytes in down link, com una massima capacità di 140

[20] http://www.weightless.org/about/weightlessn
[21] http://www.ti.com/lit/wp/swry006/swry006.pdf?DCMP=longrange&HQS=ep-wcs-lprf-longrange-contrib-whip-narrowband-wwe
[22] https://www.sigfox.com/

messaggi/giorno in uplink e 4 messaggi/giorno in downlink, nel rispetto della normativa CEPT23 sulla allocazione delle frequenze ISM24;

- raggio di copertura che va dai 3/10 Km per le aree urbane, fino ai 30/50 km per le aree rurali.
- Il numero massimo di messaggi che possono essere inviati ogni giorno è di 140.

Questa limitazione è dovuta, in parte, al rispetto delle normative del settore. La normativa europea che disciplina la banda 868 MHz consente un *duty cycle* di trasmissione del 1%. Un singolo dispositivo non potrà pertanto trasmettere per più dell'1% del tempo in un'ora. Poiché l'invio di un messaggio può richiedere fino a ~ 6 secondi, ne deriva che potranno essere trasmessi massimo 6 messaggi all'ora.

La resilienza della rete è garantita dal fatto che ogni messaggio viene ripetuto su 3 diverse frequenze dello spettro ISM ed ogni messaggio viene ricevuto da almeno 3 diverse base station. La sicurezza dei dati trasmessi viene assicurata dal fatto che il messaggio "over the air" non contiene dati che rendano identificabile l'utente.

L'utilizzo di frequency hopping, unitamente ai livelli di trasmissione quasi a livello del "background noise" e al valore di link budget rendono il sistema particolarmente robusto al "jamming" intenzionale.

I dati trasmessi sono ricevuti dalle base station Sigfox compatibili e inoltrati, tramite rete dedicata e protetta, ai server del cloud Sigfox, che verificano l'integrità dei dati e inoltrano i messaggi al sistema IT dell'applicazione corrispondente, via API.

La società ha recentemente presentato due nuovi moduli che combinano il protocollo proprietario con altri protocolli di connessione, come Wi-Fi e Bluetooth Low Energy (BLE). L'abbinamento di questi protocolli con SigFox garantirà benefici e funzionalità aggiuntive richieste dalle più diffuse applicazioni IoT.

Attualmente il sistema Sigfox copre Spagna, Portogallo, Francia, Olanda e nell'area di San Francisco, parzialmente in Italia (tramite Nettrotter), Austria, Irlanda, Regno Unito, Belgio e

[23] http://www.cept.org/
[24] ERC-REC 70-03

Lussemburgo; mentre il roll-out è previsto in Germania, Danimarca, Australia, Brasile, Repubblica Ceca, Mauritius, Nuova Zelanda, Oman e USA.

6.4. Data Link Protocol

I data protocol garantiscono la comunicazione tra la rete e lo strato applicativo. I principali protocolli di comunicazione di riferimento sono:

AMQP (Advanced Message Queuing Protocol) AMQP è un protocollo di livello binario, progettato per supportare efficacemente un'ampia varietà di applicazioni di messaggistica e modelli di comunicazione. **CoAP** (Constrained Application Protocol): progettato per garantire un protocollo applicativo RESTful, basato su semantica http, ma con footprint inferiore e approccio binario (rispetto a quello testuale). Segue il paradigma Requeste / Response asincrono. Nasce per lavorare sullo strato UDP. CoAP è semanticamente allineato con HTTP e dispone perfino di una mappatura one-to-one bidirezionale con HTTP. I dispositivi di rete sono vincolati da microcontroller di dimensioni minori con piccole quantità di memoria flash e RAM, mentre i vincoli su reti locali, ad esempio 6LoWPAN, sono dovuti a percentuali di errore di pacchetto elevate e a una bassa velocità di elaborazione (decine di kilobit al secondo). CoAP può essere un buon protocollo per dispositivi a batteria o con approvvigionamento energetico.

HTTP/HTTPS: è la base del modello client-server utilizzato per il Web. Il metodo più sicuro per implementare HTTP nel proprio dispositivo IoT è quello di includere solo un client, senza server. In altre parole, la sicurezza è maggiore se il dispositivo IoT può avviare connessioni a un server Web, ma non è in grado di ricevere richieste di connessione.

MQTT: si tratta di un sistema di messaggi che utilizza meccanismi di publish/subscribe e modelli di tipo Broker. Il footprint dei metadati è minimale (2 bytes a messaggio) ed è stato progettato per supportare contesti con connettività intermittente e con perdita di messaggi, per lavorare sullo strato TCP. Dispone di diverse librerie di supporto. Il protocollo è più difffusamente descritto nel paragrafo ad esso dedicato.

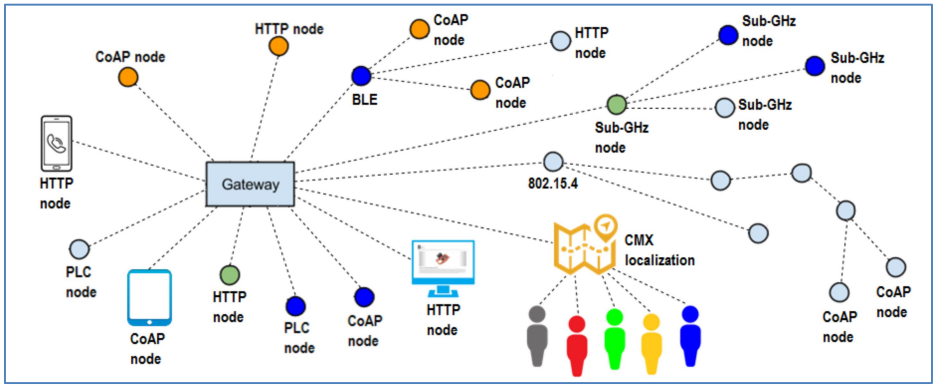


Figura 6 La babele dei protocolli[25]

Ad oggi, il protocollo HTTP risulta eccessivamente verboso per i contesti IoT, il protocollo CoAP non ha un supporto esteso in termini di librerie e comporta maggiori difficoltà rispetto ad MQTT nella gestione di eventi e nella connettività attraverso firewall e reti NAT, ma vi sono contesti in cui può essere preferibile.

Un aspetto fondamentale dei dispositivi IoT è la capacità non solo di inviare dati al Cloud o al Server, ma anche di riceverli, requisito pienamene soddisfatto dalla specifica MQTT che permette al dispositivo sia di pubblicare eventi che sottoscriversi (ad esempio a comandi di retroazione) anche dietro a firewall o via NAT. I formati di interscambio dati adottati sono XML e JSON, quest'ultimo oggettivamente più adatto per sintesi e semantica offerta.

6.4.1. *Protocollo MQTT*

MQ Telemetry Transport - MQTT[26] è un protocollo open source sviluppato e ottimizzato per dispositivi vincolati e reti a bassa ampiezza di banda, ad alta latenza o inaffidabili. È un protocollo di trasporto di messaggistica publish/subscribe estremamente leggero e ideale per la connessione di dispositivi di piccole dimensioni a reti con ampiezza di banda minima. MQTT è efficiente in termini di utilizzo dell'ampiezza di banda, è indipendente dai dati e dispone di un riconoscimento continuo delle sessioni poiché utilizza TCP. Questo protocollo è mirato a

[25] http://wott.tlc.unipr.it/site/
[26] http://mqtt.org/

ridurre al minimo i requisiti delle risorse dei dispositivi tentando al contempo di garantire affidabilità e un certo livello di garanzia di consegna con gradi di servizio.

MQTT è destinato a grandi reti di dispositivi di piccole dimensioni che devono essere monitorate o controllate da un server back-end su Internet. Non è progettato per il trasferimento tra dispositivi, né per il multicast dei dati a molti ricevitori.

Il protocollo di trasporto su internet più indicato in ambito IoT è su IP, è ad oggi il più diffuso in quanto legato alle seguenti caratteristiche:

- Semplicità di utilizzo: poichè creato come protocollo Open27 e facilmente integrabile in qualsiasi soluzione;
- Modello di comunicazione di tipo "publish/subscribe": vige un completo disaccoppiamento fra mittente e destinatario;
- Manutenzione ridotta: legata agli aspetti di robustezza del protocollo;
- Leggerezza del trasporto: minimo ingombro del protocollo rispetto al trasporto dei dati;
- Consapevolezza nella gestione delle sessioni: le connessioni vengono gestite e mantenute da specifiche di protocollo;
- Presa in carico dei messaggi: il protocollo cerca di utilizzare il meno possibile le Risorse applicative del client;
- Persistenza dei messaggi: usando specifici livelli di QoS, (Qualità del Servizio) per il recapito dei messaggi;
- Agnosticismo rispetto al tipo di dato: il protocollo non richiede alcun tipo di format di messaggio;
- Basato su Eventi: i client possono connettersi al broker e ricevere dati sulla base di eventi che sono stati generati localmente o remotamente;

[27] https://www.oasis-open.org/news/announcements/mqtt-version-3-1-1-becomes-an-oasis-standard

È fondamentale aspettarsi che a questi principali protocolli di riferimento se ne aggiungano altri con l'evoluzione degli standard. Il layer in oggetto deve comunque garantire la possibilità di aggiungere protocolli "Custom" attraverso l'uso di servizi di "proxy mediation".

6.5. Protocolli per Infrastrutture (IPv6)

I protocolli wireless finora adottati sono stati definiti e resi disponibili prima dell'apparire dell'IoT con tutte le sue specifiche esigenze e spesso mostrano carenze in merito a performance, autonomia e consumi. Si sta lavorando per un migliore adattamento di questi alle richieste di mercato e per indirizzare proposte più adeguate a creare Wireless Sensor Network (WSN) raggiungibili via Internet.

Lo scenario che si sta delineando nel mondo IoT è quello di avere:

- Reti WSN costituite da sensori IP-based che andranno in Internet direttamente tramite un edge router posto ai confini di una rete Backbone IP/MPLS, con il compito di ruotare i pacchetti verso un centro di elaborazione o di garantire un controllo remoto degli stessi sensori anche via smartphone/tablet;
- Reti WSN costituite da sensori non IP-based, dedicate per lo più a comunicazioni locali di tipo M2M, che andranno in Internet attraverso dispositivi gateway con tecnologia proprietaria con la funzione di traduzione dei diversi linguaggi in IP.

In sostanza, avvalendosi di molteplici tecnologie di comunicazione (tipicamente a corto raggio) si può creare un sistema pervasivo ed interconnesso di oggetti

Tra le tecnologie WSN spicca lo standard IEEE 802.15.4, esso è alla base di reti di tipologia LR-WPAN (Low Rate Wireless Personal Area Network): ovvero reti wireless a corto raggio, con basse velocità di trasferimento dati e a basso consumo. Queste reti sono anche definite reti "constrained": ZigBee, IEC 62591 (WirelessHart), ISA100.11a, Thread, Bluetooth ed altre tecnologie condividono questo standard.

Queste reti sono state per molto tempo ritenute troppo "deboli" per supportare lo stack TCP/IP che definisce Internet. Ma l'evoluzione nella tecnologia dei sensori ha portato cambiamenti significativi, tanto che ora è possibile usare la suite di protocolli Internet (IPv6) direttamente sulle reti IEEE 802.15.4.

L'obiettivo è integrare queste tecnologie in architetture basate sul protocollo IP, in modo tale da dare concretamente vita alla visione dell'Internet delle cose trasformando ogni oggetto intelligente in un nodo della rete Internet.

Nel seguito si presenta una sintesi del lavoro di standardizzazione svolto dall'IETF (Internet Engineering Task Force), l'ente normatore a cui si deve la maggior parte dei protocolli attualmente in uso in ambito Internet, applicato all'ambito di queste reti wireless WSN denominate LR-WPAN.

6.5.1. *IETF 6LoWPAN (IPv6 over Low power Wireless Personal Area Networks)*

IETF IPv6 Low Power and Lossy Network

Vi sono network composti da devices aventi limiti di riserva di energia e limiti computazionali, che possono inoltre essere soggetti da alta perdita dei dati, basso data rate, instabilità del segnale. Per essi possono essere adottate diverse tecnologie di comunicazione: IEEE 802.15.4, Bluetooth, Low power WiFi e PLC (PowerLine Communication).

Per il superamento di molti dei limiti di servizio il lavoro di standardizzazione è stato imperneato sulla progettazione di efficienti algoritmi di routing per i Low Power and Lossy Network. Il nuovo protocollo 6Low Power si propone di rispondere ai requisiti di sistema richiesti per la adozione su vasta scala in varie importanti aree applicativi: home e building automation, reti urbane di WSN, reti industriali di WSN.

LowPANs sono caratterizzate da

- Piccolo formato dei pacchetti, il pacchetto standard IEEE 802.15.4 è di 127 ottetti. Il frame massimo comprende 25 ottetti per l'intestazione e 102 per il MAC layer. L'aggiunta di un link layer lascia solo 81 ottetti per i dati.
- Indirizzi MAC di 16-bit fino a 64 –bit.
- Piccoli Data rate: 250 kbps, 40 kbps or 20 kbps
- Topologie di rete diversificate: star, tree e mesh

- Nodi remoti con specifiche tecniche limitate: basso costo, basso consumo di energia, limiti computazionali, non affidabilità nella continuità di servizio.
- Localizzazione casuale dei devices di campo
- Cicli di servizio variabili: i devices di campo possono essere mantenuti in stato "dormiente" per conservare l'energia e quindi non sono in grado di comunicare, se non attivati

Lo standard definisce il format del frame per la trasmissione dei pacchetti IPv6 e il metodo che deve essere usato per creare indirizzi locali e indirizzi auto configurabili "stateless" nei network basati sul IEEE 802.15.4

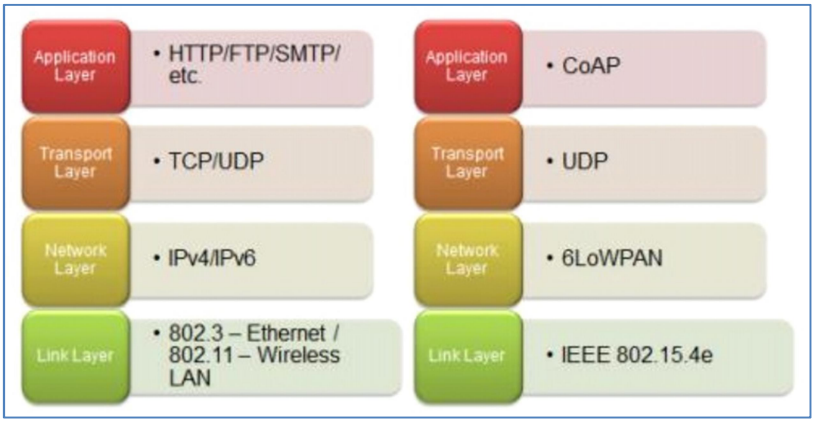


Figura 7 La variazione della suite dell'Internet Protocol

La tecnologia 6LoWPAN è elemento chiave del protocollo Thread[28], dove Thread è il nome di un nuovo protocollo wireless usato come standard per le Smart Home. Nasce grazie al Thread Group, che è un consorzio di aziende del settore e si pone l'obiettivo di semplificare al massimo la connessione tra diversi dispositivi e di superare il modello centro-stella per abbracciare le reti mesh, in cui ogni dispositivo diventa un nodo della rete. I prodotti ZigBee potrebbero diventare compatibili con il protocollo Thread con un semplice aggiornamento del firmware. Infine l'ente IETF sta continuando a lavorare per valutare e definire l'implementazione del protocollo IPv6 anche su altre tecnologie diverse dalla IEEE 802.15.4, tra cui Bluetooth Low Energy (BLE), abilitando così le connessioni dei dispositivi BLE verso internet. Bluetooth Low Energy è diventata col tempo una tecnologia importante per applicazioni, ad esempio, nel campo del

[28] https://www.threadgroup.org/

monitoraggio della salute e del fitness e per applicazioni di micro-localizzazione, identificazione e prossimità.

IETF CORE (Constrained RESTful Environments)

Il gruppo di lavoro IETF CORE ha definito il protocollo applicativo CoAP (Constrained Application Protocol) che è usato sopra il protocollo di trasporto connectionless UDP (User Datagram Protocol) e viene facilmente convertito in HTTP per un'interazione "web-like" con i nodi di sensori wireless.

Lo scopo di questo gruppo di lavoro è stato di portare l'architettura REST (Representational State Transfer, ovvero uno stile architetturale per il disegno di applicazioni di rete che usa una comunicazione tra macchine basata su richieste HTTP) nelle reti "constrained", in modo da rendere veramente possibile le interazioni con i dispositivi connessi.

I protocolli tradizionali di Internet (come HTTP e TCP) vengono già utilizzati nelle reti wireless e potrebbero funzionare anche nelle reti "constrained", ma lavorerebbero sempre in condizioni critiche mettendo in pericolo la stabilità della rete. Infatti, non sono ottimizzati per comunicazioni a bassa potenza come quelle nelle reti WSN a causa di header e meta-data pesanti e per l'esigenza di fornire alta affidabilità nelle trasmissioni, garantita dall'invio di pacchetti di conferma (packet acknowledgement). Tutto ciò consuma energia e memoria che sono risorse preziose in dispositivi a risorse limitate. In definitiva, serve un protocollo molto più leggero, come CoAP, che garantisce affidabilità nelle trasmissioni.

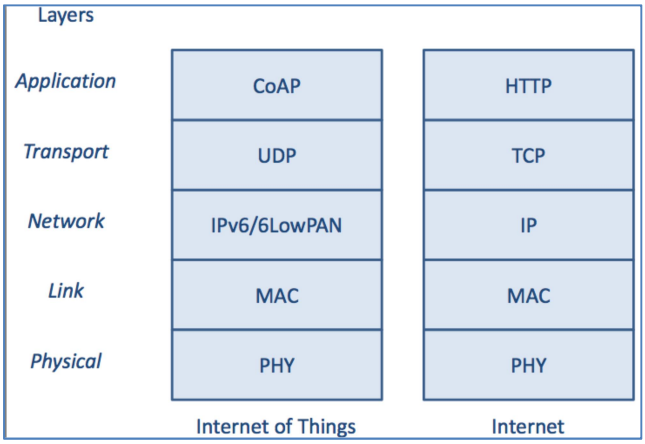


Figura 8 - Protocolli applicativi il "Web of things"

IETF ROLL (Routing Over Low Power and Lossy Networks)

Il gruppo di lavoro IETF ROLL ha sviluppato un nuovo protocollo di routing che prende il nome di RPL (IPv6 Routing Protocol for Low power and Lossy Networks). RPL è stato sviluppato appositamente per le reti di sensori. Esso deve garantire un breve percorso dei pacchetti, quindi un basso consumo di energia e deve essere a conoscenza della topologia globale della rete. Il protocollo supporta una varietà di applicazioni che spaziano dal campo industriale, urbano, home, automazione degli edifici e Smart Grid. Esso utilizza un approccio proattivo di tipo distance-vector: le informazioni di routing sono acquisite prima che sia necessario inviare un pacchetto e ai link di collegamento è associato un costo. I vari dispositivi salvano localmente le informazioni sul next hop all'interno della loro routing table.

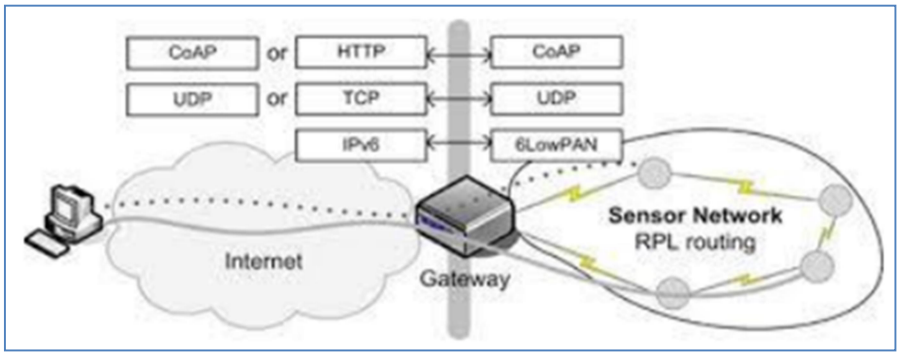


Figura 9 – Rete di sensori che utilizzano i protocolli standardizzati IETF

In questo contesto era stato sviluppato il Sistema Operativo open source con "tiny stack" denominato **Contiki**[29]**,** che permette comunicazioni Internet anche ad apparati dotati di microcontrollori con risorse limitate, supportando i protocolli standardizzati IETF (6LowPAN, COAP e RPL) per un networking IPv6 a bassa potenza nelle reti WPAN.

IETF Time Slotted Channel Hopping (6 TSCH)

L'attività di standardizzazione in corso all'interno dell'IETF, la Deterministic IPv6 over IEEE 802.15.4e Time Slotted Channel Hopping (6 TSCH) ha il compito di definire l'abilitazione del

[29] http://www.contiki-os.org/

protocollo IPv6 nello standard IEEE802.15.4e in modalità TSCH su reti di tipologia mesh. Questa attività si fonda sulle risultanze dei gruppi IETF 6LoWPAN e ROLL per una piena integrazione con essi.

Colmando una lacuna nello stack di protocolli IP, il 6 TSCH consentirà, principalmente nel mondo industriale, la creazione di reti di sensori wireless, basate su IP, interoperabili e completamente standardizzate in grado di garantire le massime affidabilità ed efficienza energetica grazie all'adozione del meccanismo di accesso al mezzo Time Slotted Channel Hopping (TSCH), alla base di standard industriali come WirelessHART and ISA100.11a.

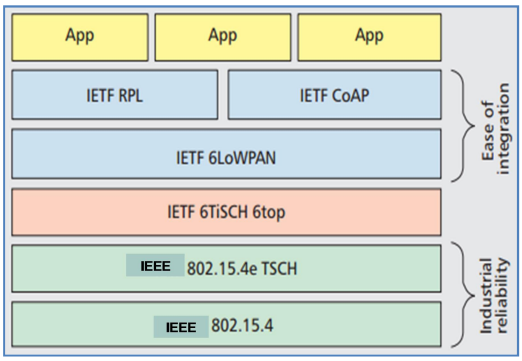


Figura 10 - Descrizione dello stack 6TiSCH

I web developer potranno richiedere dati in tempo reale dai sensori inoltrando richieste via web all'indirizzo IP di un sensore e la rete di sensori wireless sottostante supporterà tale comunicazione con un'affidabilità dei dati maggiore del 99,999%.

6.6. Funzionalità di rete, il ruolo del 5G

Nel mondo dell'IoT le applicazioni, i dispositivi e i sensori sono molteplici e con una diversità maggiore del tradizionale mondo delle telecomunicazioni mobile o fisso.

Ci sono applicazioni che fanno uso di grosse quantità di dati, altre che necessitano di bassa latenza e affidabilità come quelle basate su attuatori e sensori; alta sicurezza nella validità dei dati, come nell'industria e nell'automation. Ci sono poi applicazioni che necessitano un

controllo specifico del traffico o fanno uso di grandi volumi di segnalazioni, come per l’automotive.

La rete deve rispondere a requisiti di flessibilità, scalabilità, efficienza, global reach. Deve avere quindi la capacità di indirizzare connettività e/o business globali, di garantire la diversità di requisiti dell’IoT per servire le diverse industrie attraverso asset di reti unici e condivisi (anche nell’ottica di una shared infrastructure).

Non tutti i casi di utilizzo futuri richiederanno reti che siano ultra-veloci, super intelligenti e abbiano la capacità di sostenere un massiccio numero di dispositivi. Invece, le reti saranno costruite in modo flessibile tale che la velocità, la capacità e la copertura possano essere assegnati attraverso configurazioni software, in risposta alle specifiche esigenze di ciascun caso d'uso.

La combinazione della tecnologia “cloud distribuita” con il software-defined networking (SDN) e la “virtualizzazione delle funzioni” di rete (VNF) consente infatti la realizzazione di sistemi con un alto grado di astrazione, aumentando la flessibilità delle reti e dei servizi connessi.

Poco meno di quattro anni è l’arco temporale previsto per l'introduzione del nuovo standard delle reti di comunicazione di quinta generazione (5G), che consentirà di rimuovere molte delle limitazioni prestazionali e di servizio imposte dalle attuali tecnologie. Le nuove reti abiliteranno trasferimenti dati in modalità ultra-veloce con prestazioni stabili e sostanzialmente invarianti nel tempo e nello spazio.

La transizione da 4G a 5G può essere vista come il passaggio dalla comunicazione dei contenuti alla comunicazione delle azioni di controllo; essa consentirà di interagire da remoto e in completa affidabilità con i dispositivi più disparati, come auto, dispositivi medici, robot, droni grazie a latenze ridotte a pochi millisecondi. I principali requisiti tecnologici per i 5G indicati ad esempio da NGMN sono rappresentati in figura, ove sono riportati per confronto i valori caratteristici del 4G.

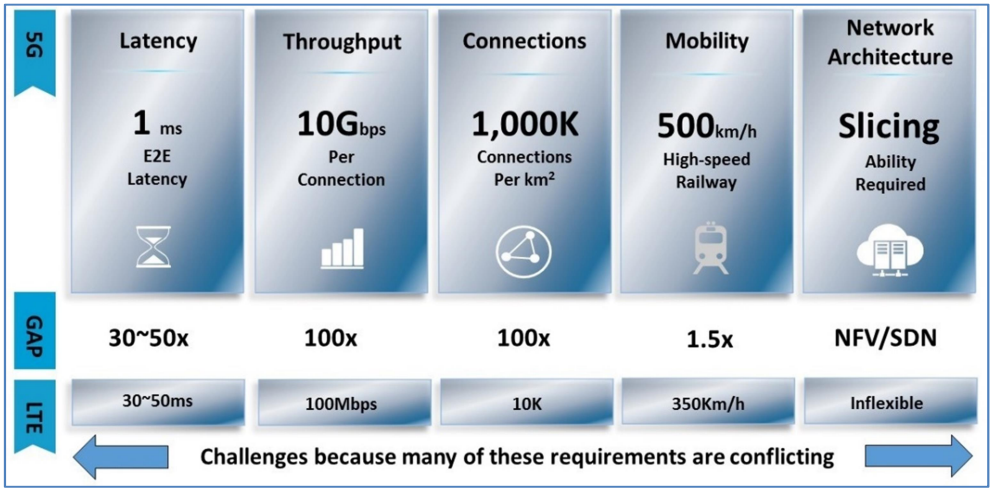


Figura 11 – Requisiti dei servizi 5G[30]

I requisiti per le reti di quinta generazione sono stati stabiliti da 3GPP[31] nell'ambito dell'attività di studio che va sotto il nome di SMARTER (*New Services and Markets Technology Enablers*), iniziata nel marzo 2015 e diviso in due fasi. Il focus della importante seconda fase sarà centrato su scenari caratterizzati da elevata velocità trasmissiva e dalla pervasività dei servizi, sui cosiddetti "Verticals", cioè tipologie di servizio caratterizzate da requisiti peculiari e molto stringenti. Particolare attenzione verrà posta al fenomeno della connessione ad Internet dei dispositivi che danno vita all'Internet of Things.

Per soddisfare i requisiti di servizio sopra citati sono da poco iniziate in 3GPP ulteriori attività di studio per la definizione di una nuova RAT (*Radio Access Technology*), in grado di sfruttare anche frequenze al di sopra dei 6 GHz (fino 100 GHz), e di una nuova CN (*Core Network*). L'attività per la definizione della nuova CN ha mosso i suoi primi passi in 3GPP nel Novembre 2015. Non è ancora noto se la nuova architettura di rete rappresenterà un'evoluzione oppure una rivoluzione rispetto alla CN 4G, perché siamo ancora nella fase in cui si stanno traducendo i requisiti di servizio identificati in SMARTER in requisiti architetturali e si sta cercando di concordare tra le varie aziende presenti in 3GPP i capisaldi sui quali si fonderà il disegno della nuova CN.

[30] Huawei (2013) 5G A Technology Vision
[31] Una nota dolente è il ritardo previsto in Italia nella liberazione della frequenza base (circa 700MHz), oggi in uso nelle TV commerciali private. Un ritardo di circa 2 anni sulla Europa.

E' stato comunque stabilito che la nuova CN dovrà supportare nativamente non solo LTE Advanced (evoluzione dello standard Long Term Evolution) e il nuovo RAT 3GPP cui si accennava sopra, ma anche tipologie di accesso non-3GPP, quali il Wi-Fi. Ovvero si dovrà realizzare in modo nativo la convergenza fisso mobile e ciò dovrà consentire ad un terminale, che utilizzi contemporaneamente diverse tecnologie di accesso, di instaurare connessioni multiple simultanee a una molteplicità di servizi estremamente eterogenei, sia in termini di velocità di trasmissione (si va dagli svariati Mbit/s dello streaming video ad alta definizione ai pochi bit al giorno o al mese) sia in termini di Qualità del Servizio. In particolare la nuova piattaforma di telecomunicazione 5G, attraverso la virtualizzazione e l'astrazione delle risorse di rete consentirà efficientemente di introdurre il meccanismo di Network slicing. Il network slicing permetterà, a partire da un'unica rete fisica, l'istanziazione logica di reti (slices) con le caratterizzazioni funzionali e prestazionali richieste per l'erogazione degli specifici servizi verticali IoT.

Con il "network slicing" una rete si potranno creare reti parallele attraverso una definizione software delle funzionalità di rete di nodi virtuali quali per esempio l'MME, SGW and PGW[32] per garantire e caratterizzare i livelli di servizio e le prestazioni di rete, quali la mobilità, la copertura, il data rate, la latenza, l'affidabilità. Tutto ciò consente di abilitare così nuovi e più efficienti modelli di business.

Inoltre le reti 5G abilitano una efficace separazione tra piano di controllo e piano di utente della rete stessa consentendo una scalabilità indipendente dei due piani introducendo un altro grado di flessibilità. Per esempio un'applicazione che necessità funzioni di user plane a basso ritardo possono essere erogate vicine all'accesso, mentre le funzioni di control plane possono essere poste in maniera più centralizzata.

I benefici che comporterà la nuova infrastruttura di rete rispetto a quella tradizionale, basata su HW dedicato sono molteplici; innanzitutto una "capital efficiency" grazie all'uso di HW commerciale "off-the-shelf" (COTS), per fornire le funzioni di rete attraverso la tecnica della virtualizzazione (Virtualised Network Functions, VNFs). Poi la condivisione di risorse HW e la semplificazione delle differenti architetture di rete. Ciò abiliterà alla:

[32] Entità preposte al controllo della mobilità MME (Mobility Management Entity) e dei nodi di trasporto: SGW (Serving Gateway), PGW (PDN Gateway).

- flessibilità nell'uso delle risorse HW;
- scalabilità di sistema e disaccopiamento delle funzioni di rete dal sito geografico;
- rapida innovazione dei servizi, attraverso uno sviluppo software-based;
- aumento dell'efficienza operativa realizzata attraverso procedure comuni di automatizzazione e operatività;
- ridotto consume energetico;
- Interface standard e aperte (open interfaces) tra le funzioni di rete virtualizzate e l'infrastruttura e le entità di gestione associate.

6.7. Network management & orchestration

A questo componente architetturale è demandata la gestione delle varie parti di sistema relativamente: al suo funzionamento, manutenzione, amministrazione; alla gestione dei dispositivi, delle reti di comunicazione, dei dati di configurazione e provisioning, alla configurazione dei servizi forniti, ecc.
Considerata la peculiarità del mercato IoT, in rapida crescita, caratterizzato da ampi volumi di dispositivi connessi, da marginalità ridotta rispetto a quella del mercato delle comunicazioni tradizionali (fonia) e considerando i modelli di business e di GTM (Go to Market) con cui si offrono i servizi IoT, è chiaro che i tradizionali sistemi BSS (Business Support System) e OSS (Operational Support System) non sono la soluzione migliore per la strategia IoT. Di seguito alcuni esempi.

- SIM lifecycle management: il lifecycle tradizionale (consumer-oriented SIM card lifecycle) non è adeguato alle soluzioni IoT; pertanto il layer di management dovrà supportare un lifecycle management specifico per l'IoT in cui molti controlli, per esempio sul SIM management, sono forniti direttamente al cliente in modalità self-service;
- Device management: la configurazione dei dispositivi/sensori IoT e la gestione delle soluzioni richiede l'integrazione con i sistemi OSS;

- Il provisioning e l'attivazione dei servizi IoT richiedono la caratterizzazione e l'ottimizzazione dell'uso delle risorse di rete al fine di garantire un adeguato livello di servizio e evitare un inutile sovraccarico dei sistemi e delle reti dei service providers;
- Charging and billing: l'IoT richiederà sempre di più la possibilità di gestire il Real-time charging, la policy control, la condivisione della banda tra più utenti IoT. Quindi i sistemi di charging e billing IoT dovranno essere sufficientemente avanzati e scalabili;
- Fraud management: l'IoT richiede un robusto sistema di rilevamento delle frodi (fraud detection) per garantire che i devices/sensors e l'infrastruttura IoT non siano compromessi intenzionamente o involontariamente;
- Resource inventory: tipicamente i sistemi di inventory tradizionali conservano dati minimali; basti pensare ai dati relativi alle SIM cards; le IoT applications richiedono un modeling dei servizi e delle risorse usate (come le SIMs e i devices), quindi l'inventory necessaria sarà più ricca e complessa;
- Self-administration: i servizi IoT di default richiedono un elevato grado di self-administration. Questo è realizzato attraverso sistemi automatizzati che limitano l'intervento del cliente. Ovviamente ciò implica una rivisitazione dei processi di business e operation tradizionali.

6.8. Edge Computing

Parte dei dati generati dalle applicazioni IoT necessità di essere eleborato a livello della rete Edge (su router, mobile device, appliance, etc.). Un modello imposto dalla necessità di avere una latenza (tempo necessario per trasferire le informazioni al centro e viceversa) relativamente breve, di ridurre i costi di trasporto, di permettere una elaborazione locale dei dati.

L'implementazione di una soluzione di Edge Computing comprende prodotti per:

- la connettività di rete;
- la sicurezza fisica e cyber-security;
- lo sviluppo di applicazioni Edge;

- l'analisi dei dati;
- la gestione e l'automazione.

I vendor si stanno sfidando su questo fronte e hanno come obiettivo il rilascio di soluzioni aperte per il mercato IoT che si installano alla periferia della rete consentendo ai clienti di aggregare e analizzare i dati in tempo reale e di monitorare dispositivi e cose. Questi sistemi sono adatti a una grande varietà di applicazioni industriali, logistiche, retail, per i trasporti, per la sanità, per la pubblica amministrazione, etc.

7. Service e Application Layer

Il concetto di IoT si è evoluto nel tempo e ha ormai raggiunto un buon grado di maturità; da singole sperimentazioni in ambiti specifici si è passati ad una logica sistemica, la quale vuole favorire l'integrazione tra dispositivi/sensori e applicazioni diverse.

L'Internet of Things, per natura trasversale, include diverse aree:

- Reti wireless di sensori e attuatori;
- Wearable connessi a Internet;
- Sistemi embedded a basso consumo energetico;
- Sistemi RFID;
- Interazione fra mobile device e realtà circostante;
- Smart Home;
- Connected Cars.

È quindi evidente che risulta necessario affrontare le singole soluzioni IoT con architetture modulari e scalabili che permettano di assemblare la piattaforma più adatta al singolo contesto, aggiungendo e sottraendo funzionalità. L'applicabilità di comuni soluzioni in settori diversi e la replicabilità di soluzioni di successo sviluppate in determinati contesti, richiede

quindi una trasformazione dal mondo connesso M2M, basato su applicazioni verticali, a una innovativa logica in cui un layer comune di servizio ("IoT Service support and Application layer") realizza le interazioni comuni tra i dispositivi/gateways IoT e stabilisce la comunicazione con le applicazioni. La comunicazione dei gateways e dei devices con questo layer è "IP based" e agnostica del tipo di connettività (cellular, fiber, Wi-Fi etc.) e dei protocolli di trasporto (UDP/TCP). L'IoT Service support and Application layer interagisce con le specifiche appliczioni IoT attraverso l'esposizione di standard API's.

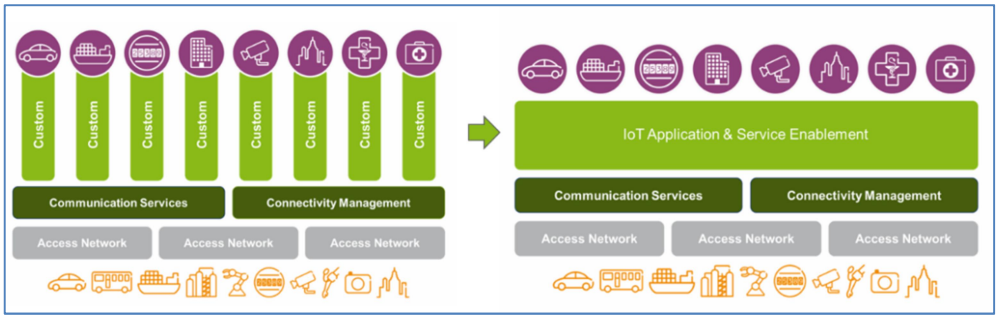


Figura 10 Mondi applicativi dell'IoT

Un tipico esempio di uso delle piattaforme che implementano il layer di "IoT Service support and Application layer" è quello delle Smart Cities: in cui le diverse applicazioni della smart city: Gestione della mobilità e dei trasporti; gestione dei servizi per l'ambiente e il suo monitoraggio; Gestione dell'energia (dalla produzione al consumo, al suo risparmio) possono essere abilitate da un'unica piattaforma di delivery dei servizi Questa sarà in grado di elaborare le informazioni trasmesse dai sensori per erogare servizi a valore aggiunto per i cittadini, contribuendo a migliorarne la qualità della vita.

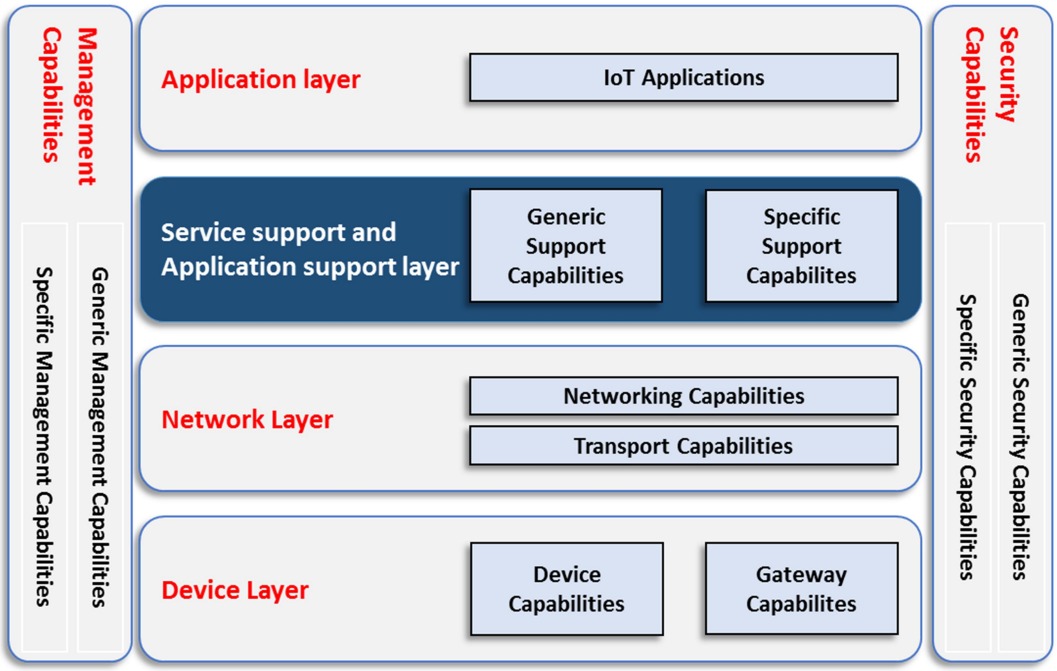


Figura 12 Service support and Application layer

Con riferimento alla Reference Architecture ITU-T sono individuati due tipologie di capability per il layer di "*Service and Application Support*":

- Generic support capabilities: le capacità di supporto generiche sono funzionalità trasversali che possono essere utilizzate in differenti applicazioni IoT come data processing o data storage. Queste funzionalità possono anche essere invocate da funzionalità specifiche dello stesso layer;
- Specific support capabilities: le funzionalità dedicate alla fornitura di servizi caratteristici per quelle applicazioni aventi requisiti specifici.

È infine da tener presente che la stessa architettura è dinamica e a fronte della maturazione di tecnologie essa stessa deve evolvere. Quello che sempre più è evidente è che i Layer Application e Service/Support entrano in contatto direttamente con il Layer dei Device. Il primo integrando ad esempio APP che accedono alla configurazione del device, il secondo attraverso agent che acquisiscono sempre più funzionalità: dalla gestione di livelli locali di elaborazione dei dati a capcità di restituire un feddback di retroazione. Riprendendo il tema

della smart city, il layer di "IoT Service Support & Application Support" potrà contenere in maniera trasversale, per esempio: l'App store per i cittadini; l'interconnessione logica delle centrali di controllo; la dematerializzazione dei processi e dei documenti; l'integrazione e l'interoperabilità dei servizi; l'abilitazione di nuovi sistemi di pagamento, dei sistemi di identificazione; la gestione sicura degli Open Data e altro ancora.

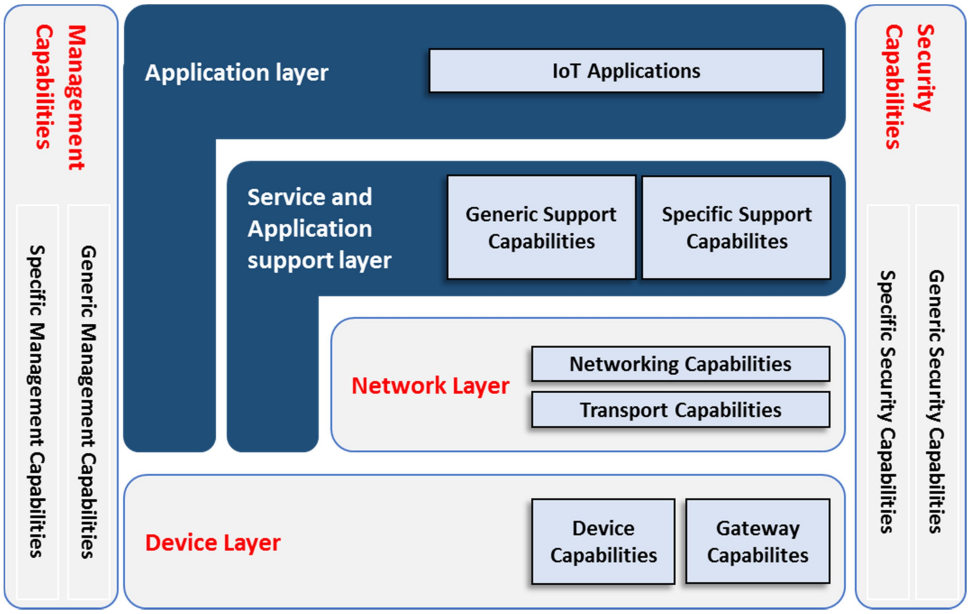


Figura 13 Interazione fra Device e Application Layer e Service/Support Layer

La Reference Architecture deve essere neutrale rispetto ai Vendor, ma influenzata dalle soluzioni migliori del mercato e delle community. La Reference Architecture deve affrontare molteplici aspetti dal cloud all'infrastruttura server-side che permette di monitorare, gestire, interagire e processare i dati provenienti dai dispositivi che possono comunicare solo grazie ad un adeguato modello architetturale; oltre agli agenti software e relativo codice.

Dal punto di vista delle capability, la Reference Architecture deve quindi tenere in considerazione i seguenti elementi:

- Connettività e comunicazione;

- Gestione dei dispositivi;
- Collezione dati, analisi (anche predittiva), attuazione ed esposizione;
- Scalabilità e Alta affidabilità;
- Sicurezza;
- Integrazione;
- Modelli di attivazione dei servizi e delle infrastrutture (cloud);

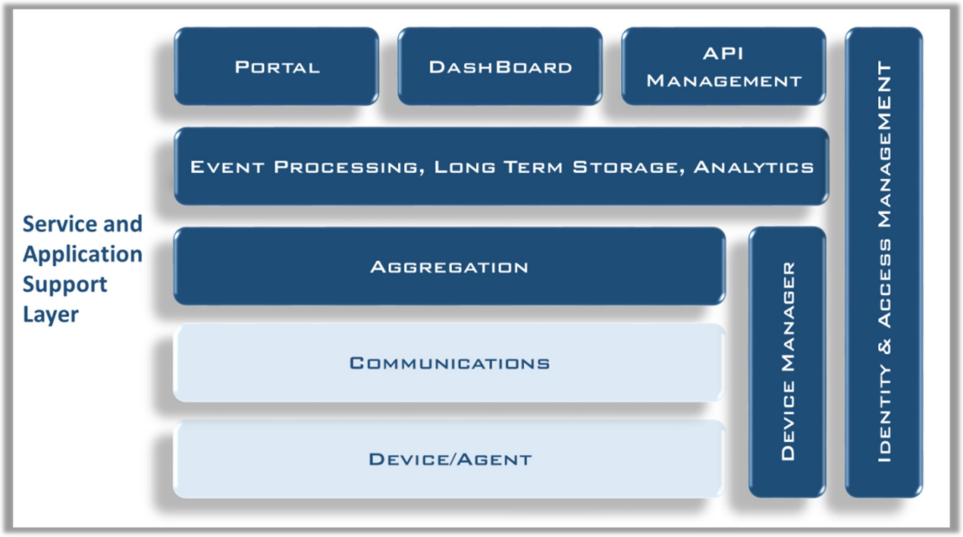


Figura 14 Componenti del "Service and Application Support Layer"

Il layer "Service Support and Application Layer Support" si pone come livello di intermediazione fra le varie componenti, deve quindi prendere in considerazione tutti questi aspetti nell'ottica di una componibilità dell'architettura operativa specifica di contesti specifici Nel layer sono inseriti, per enfatizzare gli aspetti di interazione tra i layer, i componenti "Device" e Communication, pur essendo questi parte rispettivamente del Device o Network Layer.

7.1. Architetture EDA e SOA

Un sistema IoT deve essere in grado di erogare servizi in maniera efficiente "by design" in presenza di eventi complessi e nello specifico all'interno di scenari caratterizzati da eventi ove il fattore tempo e la elaborazione real time o near real time sono fondamentali.

In questo tipo di applicazioni assumono un ruolo fondamentale le architetture guidate da eventi. La EDA (Event Driven Architecture) è l'architettura di riferimento per il mondo IoT che si affianca a quella usuale denominate SOA (Service Oriented Architecture) utilizzate nelle logiche di integrazione di servizi applicativi (Web Services) in una logica di richiesta ed esaudimento dei servizi orientati al WWW.

Entrambe le Architetture suddette vengono impiegate diffusamente poichè soddisfano i seguenti requisiti non funzionali:

- Velocità
- Elaborazione di eventi complessi
- Altà disponibilitò dei servizi
- Elasticità
- Robustezza
- Indipendenza dal formato dei dati
- Sicurezza.

Le architetture EDA sono basate sul concetto di Message Broker per lo scambio di messaggi, che sono di complemento rispetto a quelle SOA, in quanto permettono di gestire eventi complessi inerenti alle più disparate fonti di dati presenti nel contesto IoT (computer, sensori, attuatori, microcontrollori, …). L'utilizzo di architetture EDA consente di rilevare in "tempo reale" il cambiamento di stato di oggetti (e di dati) disseminati e, di conseguenza, di generare eventi che possono essere elaborati dalle componenti di servizio rese disponibili dalla integrazione di business logic ottenute secondo il paradigma SOA (Web Services, HTTP/REST, etc.)

Alla base della filosofia di comunicazione delle piattaforme IoT vi sono quindi i Message Broker che implementano meccanismi di scambio di messaggi (sincroni ed asincroni) in grado garantire una:

- Interazione fra applicazioni che sono "debolmente accoppiate "
- Persistenza del dato

- Gestione transazionale dei dati
- "Delocalizzazione" delle applicazioni
- Asincronicità nella gestione dei messaggi
- Robustezza rispetto ai fallimenti del SW
- Intermediazione frai destinatari di informazioni in quanto non devono avere consapevolezza delle reciproche caratteristiche per stabilire una corretta comunicazione fra di loro.

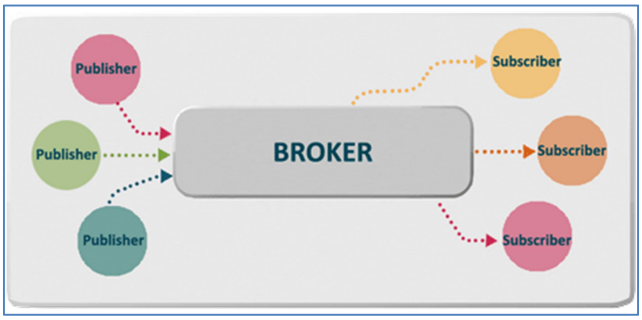


Figura 15 Message Broker

7.2. Gestione dei dati

La produzione di migliaia di eventi al secondo da parte di un vasto numero di apparati, H24 e 7 giorni su 7, richiede sistemi estremamente scalabili in grado di gestire dati di diverso tipo (strutturati e non), in real time e a lungo termine. La necessità di disporre di azioni in near real time richiede la presenza sia di sistemi di Bulk Analytics che di Event Processing e di Storage ad altissima capacità e tolleranti rispetto a sintassi troppo stringenti. Sempre più la geolocalizzazione dell'origine del dato è elemento fondamentale nella soluzione complessiva. Le componenti principali risultano quindi:

- Data Storage altamente scalabili column-based per la persistenza dei dati relativi agli eventi. Questa funzionalità può anche normalizzare i dati in data models.
- Engine basati su meccanismi di Map Reduce per batch long-running per l'elaborazione dei dati (analytics e algoritmi predittivi)
- Complex Event Processing per processare eventi in memoria in near real time

- Soluzioni di processamento dati Real-time, come per esempio dei "Rule engine" in grado di creare e gestire alarm triggers. Le "regole" possono essere basate su valori discreti o aggregati basati su localizzazione, tipo di device, tipo di sensore, tags, ...
- Linguaggi leggeri di scripting (Node.jx, PHP), Java e C come complemento per implementazioni di Agent e supporto per piattaforme tradizionali.
- Sistemi di Aggregazione di Dati (per sensori, tag, locazione) per abilitare un accesso rapido ai dati aggregato
- Sistema GIS (Graphical Information System)
- Sistema di acquisizione di 3rd party data

Gli stessi dispositivi possono disporre tramite Agent di alcune di queste capability, in particolare l'event processing, che permette l'elaborazione deidati e utilizzo di regole per attivare: alert, invio e trasformazione dati e retroazione. I sistemi di Analytics e GIS possono essere anche parte della soluzione Applicativa.

7.2.1. *Qualità del dato nel contesto IoT e Open Data*

La qualità dei dati è un aspetto estremamente critico e va valutata su vari livelli.

Si parte dalla qualità del dato acquisito e dai metadati che descrivono le condizioni di acquisizione dello stesso. È indispensabile che il sensore segnali se il dato trasmesso sia stato registrato in una situazione di funzionamento certificata, oppure no.

Una volta che il dato è stato acquisito da una piattaforma è indispensabile garantire che sintassi e semantica del dato siano ben comprese dalla piattaforma, in modo che tali dati possano essere aggregati e confrontati con dati provenienti da altri contesti.

Infine sistemi di controllo che applichino una serie di regole di audit sui dati acquisiti possono supportare l'individuazione di pattern anomali e quindi di fonti dati di bassa qualità o di interpretazioni inconsistenti

Le architetture EDA oggi largamente impiegato nelle soluzioni IoT, sono basate su un approccio a scambio di messaggi ("publish" "subscribe") e consentono in maniera agevole di prelevare

alla fonte dati sotto forma di eventi o misure, effettuare analytics, analizzarne la qualità e integrarli con altri dati presenti ad esempio nel contesto Open Data, che trovano in ambito IoT uno scenario di enorme valorizzazione, purchè ricondotti agli stessi principi di qualità ed esposti in modo che siano effettivamente fruibili anche a costo dell'applicazione di una fee a beneficio di chi garantisce un servizio di qualità sia in temirni della qualità dei dati che della semplicità di accesso.

Tale utilizzo di tecnologie in ottica IoT determinerà fortemente il successo nell'utilizzo degli Open Data e qualora non veniga considerata potrebbe quasi certamente determinare problemi di eterogenità dei dati che ha ricadute su:

- Crescita dei costi delle soluzioni
- Influenza negativa sui processi decisionali
- Impedimenti nel rapido re-engineering dei sistemi
- Diifficili strategie di integrazione di sistemi IoT e dati (a lungo termine)

È di fondamentale importanza nella analisi della qualità del dato desumere correttamente il valore reale dei dati in termini di:

- Accuratezza (vicinanza del dato ad un valore nel dominio di definizione considerato corretto)
- Correttezza (accuratezza al grado massimo)
- Completezza (l'estensione con cui i valori sono presenti nella base di dati.)
- Tempestivita (adeguatezza dell'aggiornamento)
- Consistenza (semantica di differenti valori in virtu' delle regole condivise)

E per quanto riguarda il formato dei dati è altrettanto fondamentale comprendere la loro:

- Appropriatezza (rispetto alle esigenze dell'utente o dell'applicazione specifica)
- Interpretabilità (per interpretare i valori correttamente)
- Portabilità, o Universalità (tra diverse tipologie di utenti o applicazioni)
- Precisione (capacità di discriminare tra diversi valori)

- Flessibilità (rispetto ai requisiti)
- Capacità
- Uso efficiente della memoria

La qualità del dato nel contesto *Open Data* deve essere misurabile e nei sistemi cooperativi è quindi ancor più fondamentale in quanto i destinatari o i fruitori sono gli enti esterni, per cui deve essere chiaro in partenza che nella integrazione di informazioni accada che:

- Sistemi eterogenei implicano una elevata probabilità di avere schemi logici differenti
- La necessità di scambiarsi dati può determinare l'insorgere di problemi nello scambio
- Maggiore latenza del sistema cooperativo dovuto alla catena di elaborazione e trasformazione

Per mitigare il più possibile questi rischi, e quaindi per il miglioramento della qualità dei dati possono essere impiegate le usuali metodologie che fanno uso di:

- Ispezione e correzione, mediante:
  - Comparazione dati con le controparti reali
  - Confronto di dati all'interno di più repository di dati o Database
  - Utilizzo di regole di business opportune
- Controllo e Miglioramento del Processo
- Reingegnerizzazione dei Processi

7.2.2. *Esposizione dei servizi IoT verso il layer applicativo*

I layer di supporto è inoltre responsabile di esporre i dati al layer applicativo (grezzi, aggregati o elaborati) e permettere l'interazione con i servizi IoT di supporto per la loro attivazione e configurazione:

- È possibile realizzare ed esporre front-end web based (o portali multicanale) per interagire con i servizi esposti dallo strato di supporto (event processing, analytics, device management, IAM) e con i device.

- Sono presenti dei Cruscotti statici o dinamici (Dashboard) che vengono esposti sia a fini di monitoraggio che di analisi.
- È possibile interagire con la piattaforma di supporto attraverso API sia per l'interazione con le applicazioni IoT che con sistemi terzi, anche Legacy. Le API sono gestite e controllate attraverso un sistema di API management che fornisce accesso alle API del sistema per gli sviluppatori delle applicazioni IoT, oltre a servizi di access control, throttling, routing e load-balancing. L'accesso ai dati da parte delle applicazioni (mobile apps, web, integration software etc.) sono gestate tramite APIs (Client API or OData API) attraverso richieste sicure e gestite sul controllo dell'accesso di utente. L'identità dell'utente può essere gestita attraverso identità federate e integrate con soluzioni di gestioni di credenziali integrate che usano SAML/OAuth.

7.3. Gestione dei dispositivi (Device Manager, Agent)

La gestione dei dispositivi è effettuata attraverso un sistema Server, il Device Manager (DM), che comunica con i dispositivi tramite vari protocolli e fornisce funzioni di controllo sia bulk che individuali. Inoltre deve anche essere in grado di effettuare la gestione remota del software (ed eventualmente del firmware) presente sul dispositivo, interagendo con agent software presenti sul dispositivo stesso.

Il DM gestisce la lista delle identità dei dispositivi e li mappa ai relativi proprietari, interagendo con lo IAM (Identify Access Management) per implementare il controllo d'accesso.

Si possono prendere in considerazione tre tipi di dispositivi:

- Fully Managed: integrano un agent completo attraverso il quale il DM è in grado di:
    - Gestire il software presente sul device (aggiornamenti Firmware & application)
    - Abilitare o disabilitare funzionalità (sensori, camera, …)
    - Gestire aspetti di sicurezza e aggiornare le relative credenziali
    - Monitorare lo stato del device
    - Mantenere l'informazione sulla posizione dei device
    - Bloccare o effettuare una cancellazione completa del device

  - Riconfigurare remotamente vari parametri tra cui: WIFi, GPRS, …

- Non Managed: possono comunicare con il resto della rete, ma non hanno agent. Il DM può gestire informazioni sulla disponibilità e posizione dei dispositivi, se fornita dagli stessi. Fanno parte di questo perimetro i dispositivi 8-bit che non hanno le risorse per supportare un agent.
- Semi Managed: implementano solo parte delle funzionalità disponibili sul DM.

7.3.1. *Device/Agent*

I device (o dispositivi) possono essere di diverso tipo, ma per essere considerati IoT device, devono possedere meccanismi di comunicazione che direttamente o indirettamente li mettano in contatto con la rete. Dispositivi con connessione diretta sono tipicamente gli Smart Gateway, come ad esempio un Raspberry Pi connesso via Ethernet o WiFi, dotati di indirizzo IP. Dispositivi con connessione indiretta sono ad esempio dispositivi che comunicano via Bluetooth Smart (Bluetooth Low Energy) con un cellulare o uno Smart Gateway.

Ogni dispositivo necessita un'identità che può essere che può essere un UUID (Universally Unique IDentifier) integrato nel device a livello hardware o generato dal sottosistema radio, oppure un token OAuth2[33] o ancora un identificativo salvato su una memoria non volatile EEPROM.[34]

7.4. Sicurezza nel contesto IoT

La sicurezza deve essere parte integrante e deve coprire interamente tutti i layer di servizio, solo ottenendo una sicurezza omnicomprensiva sarà possibile garantire una copertura in sicurezza dell'intera infrastruttura realizzata.

Qui di seguito una sintesi dei principi generali da tenere in considerazione per la fase di progettazione e la messa in sicurezza in termini di servizio:

[33] OAuth2 è un framework autorizzativo che permette alle applicazioni l'accesso condizionato all'User Account.
[34] Electrically Erasable Programmable Read-Only Memory, è un tipo di memoria non volatile

- I servizi di sicurezza devono essere modulari e configurabili secondo esigenze specifiche, in riferimento alle macro categorie "Massive IoT" e "Critical IoT", del servizio che s'intende realizzare e supportare definendo i principali punti di riferimento, scopi e punti di forza.
- L'architettura deve essere disegnata dividendo i diversi componenti e sotto-componenti per consentire la realizzazione di una struttura modulare. Una architettura modulare oltre ad incrementare il livello di sicurezza è abilitante in termini di efficienza e rapidità nella esecuzione e semplicità di gestione.
- Sulla base delle esigenze inerenti gli elementi principali del servizio, la sicurezza dovrebbe essere pensata e calata in ogni singolo componente per soddisfare i requisiti del rispettivo nodo (IoT, Cluster IoT, DB, LDAP, RADIUS …).
- Prevedere di adattare l'architettura anche per quelle componenti nativamente sprovviste. Per esempio, mappare l'architettura anche su diverse sotto unità (IoT, cluster di IoT e IoT Adapters…).
- Gli elementi di gestione della sicurezza devono consentire la distribuzione di tutte le risorse sensibili (Sensitive Data - Sensitive Function) e altresì consentire la configurazione e l'estensione dei servizi di sicurezza stessi.
- L'accesso all'interno dell'ambiente del servizio realizzato deve essere protetto tramite uno strato sicuro (Strong Authentication, anche basata su Inherence Factor) per garantire la riservatezza di tutte le risorse sensibili contenute.
- Tutte le risorse umane impiegate devono far parte integrante della soluzione e devono rispondere puntualmente a procedure e processi di sicurezza in grado di mantenere costante il livello di sicurezza implementato.

La sicurezza si esplica in generale in informatica applicando i concetti di *disponibilità, integrità e riservatezza* delle informazioni gestite. Nel caso dei sitemi presenti nel contesto IoT tali concetti si applicano similmente con opportuni distingui o accortezze aggiuntive inerenti alle tecnologie impiegate, ai domini di rete, alle applicazioni erogate ed alle risorse dei sistemi (device) in essi disponbili.

Le proprietà di base su cui si fa riferimento.

- Riservatezza: è la proprietà per cui l'informazione non è resa disponibile a soggetti non autorizzati.
- Integrità: è la proprietà di inalterabilità dell'informazione (sia che essa venga scambiata sia che venga memorizzata e successivamente recuperata)
- Disponibilità: proprietà di gestione controllata del flusso delle informazioni.

Quest'ultima è attuata mediante la esecuzione dei seguenti processi:

***Autenticazione*:** è la verifica dell'identità dei dispositivi, delle utenze, delle applicazioni.

Autorizzazione*:** è la determinazione se ad un soggetto, che richiede dati e/o servizi, in generale l'accesso ad una risorsa, è permesso il diritto a fare quella richiesta. ***Non Ripudio: è la proprietà per cui il destinatario di una comunicazione può provare che il mittente effettivamente abbia effettuato la comunicazione, anche se quest'ultimo successivamente volesse negare di averla mai effettuata ***Auditing:*** è l'azione di registrare, in modo permanente e non modificabile, tutte le richieste (e rispettive risposte) effettuate dai soggetti al sistema o tra di loro.

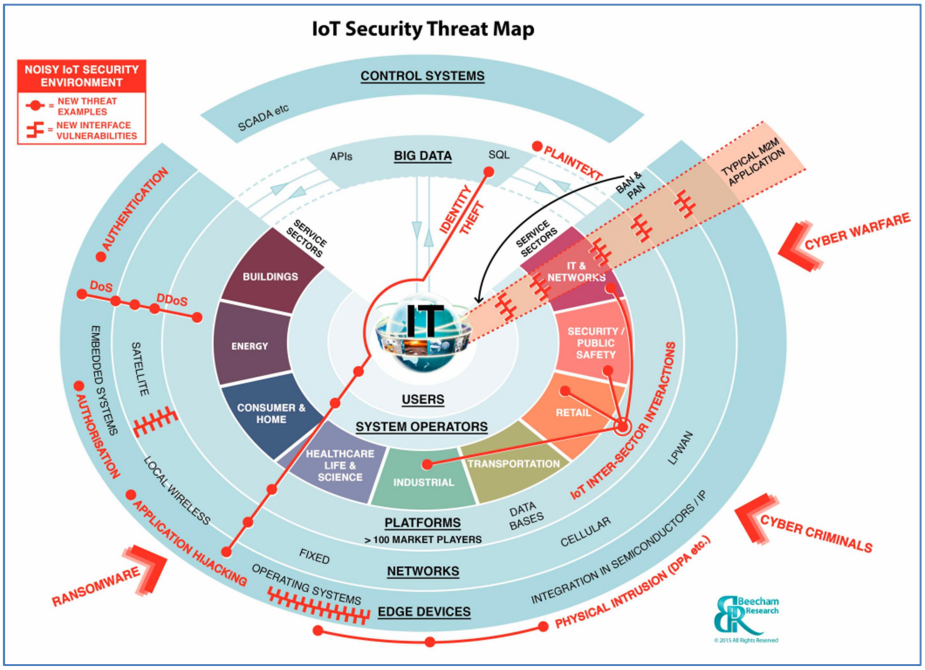


Figura 16 IoT Security Map[35]

Gli Eventi Indesiderati, ovvero gli attacchi a livello logico nel contesto ICT e IoT sono principalmente tesi a sottrarre informazione o degradare la operatività del sistema, sono possibili quattro categorie di attacchi:

- Interruzione. Una parte del sistema viene distrutta o diventa non utilizzabile. Questo è un attacco alla disponibilità del sistema.
- Intercettazione. Un soggetto non autorizzato ottiene accesso ad una componente del sistema. Questo è un attacco alla riservatezza (sniffing, spoofing, password cracking)
- Modifica. Un soggetto non autorizzato entra in possesso di una componente del sistema, la modifica e la introduce di nuovo nel sistema. Questo è un attacco all'integrità.
- Produzione. Un soggetto non autorizzato produce componenti nuove e le immette nel sistema. Questo tipo di attacchi può essere meglio prevenuto avvalendosi di sistemi di

[35] Beecham Research IoT Security Map, 2015

device management specifici per il contesto IoT e che tengono sotto controllo l'intera flotta di dispositivi disseminati.

Gli attacchi alla sicurezza ICT possono essere quindi svariati e nel contesto IoT molto più subdoli ed articolati poiché nella loro complessità oltre alla dimensione logica si aggiunge anche quella fisica (tampering) in quanto i device stessi possono essere soggetti a manomissioni quando disseminati in ambienti esterni non sottoposti a controllo. Il tampering è la tecnica mediante la quale si possono operare modifiche o interruzioni di funzionalità sui device agendo esternamente ad esso oppure manomettendone localmente il firmware (sw a bordo del device).

In un contesto di sistemi distribuiti come l'IoT, in cui la rete diventa un elemento fondamentale, si può parlare di sicurezza indicando l'insieme di procedure, pratiche e tecnologie per proteggere le risorse, gli utenti e le organizzazioni che operano mendiante tali infrastrutture. Un approccio sistematico alla sicurezza di rete nel mondo IoT (rete di sistemi) la implementazione di *Meccanismi (o*gni soluzione progettata per scoprire, prevenire e recuperare un attacco) e di S*ervizi (*ogni servizio dedicato alla sicurezza del sistema e delle informazioni in transito).

Alcuni principi guida:

- Adottare il principio Privacy by design per analizzare i bisogni per la sicurezza e la privacy degli utenti
- Adottare approcci di sviluppo delle piattaforme e delle applicazioni che soddisfino i principi dei Trust tra layer, trust tra layer e piattaforme e trust tra oggetti.
- Implementare soluzioni per la sicurezza del layer fisico e per la sicurezza delle comunicazioni (crittografia)
- Fare riferimento agli standard e alla best practices
- Definire il ciclo di vita degli elementi hardware e software del sistema
- Definire modelli di autenticazione / autorizzazione anche durante lo sviluppo del software

- Definire ed implementare un framework per l'identity management e la supervisione anche nel più ampio ecosistema di servizi IoT.

Ne risulta che a seconda delle circostanze e quindi dei tipi di device impiegati in IoT, si possono impiegare differenti meccanismi di sicurezza della rete e dei dati trasportati:

- Tecniche crittografiche: algoritmi di crittografia dei canali di comunicazione dei dati per la confidenzialità e la firma digitale. (HASH, HMAC, SHA1, SHA2, RSA, AES, 3DES, etc)
- Protocolli sicuri: IPSEC suite, Transport Security Layer (DTLS, TLS v1.2, etc)
- Firewall: per la protezione degli end point, dei servizi esterni ed interni e delle applicazioni (IDS, IDP, etc.)
- Sistemi NAC (Network Access Control): Sistemi di controllo di accesso alle reti ed ai servizi interni mediante protocolli specifici di autenticazione (Radius, Kerberos, etc.)

I servizi per la security che possono essere implementati devono essere funzionali, pur in una ottica complessiva, al segmento architetturale servito.

7.4.1. *Security per gli oggetti "Critical IoT"*

Per tutte le infrastrutture che prevedono l'impiego di "Critical IoT" dovranno essere predisposte funzionalità e soluzioni per garantire la sicurezza by design, durante tutte le fasi prima e dopo il trasporto delle informazioni. Tipicamente per lo scambio di messaggi tra due entità IoT non è fondamentale che questi siano autenticati. L'autenticazione è richiesta sulla base della tipologia delle informazioni in transito tra due sistemi IoT o dalla criticità di un sistema centrale. L'attività cardine per stabilire tale criticità sarà l'analisi sulla classificazione delle informazioni. Soltanto dopo aver stilato questa classifica e stabilito il livello di sicurezza da adottare sarà possibile stilare un programma sul livello di autorizzazione, funzionale alla categoria di IoT trattata (Massive o Critical IoT).

Tra gli oggetti "Critical IoT" dovranno essere eseguite previste le seguenti componenti e/o funzioni:

- Le chiavi crittografiche per garantire l'autenticità della fase di autorizzazione;
- Le chiavi crittografiche per consentire l'autenticazione tra le due entità IoT-2-IoT (M2M);
- la salvaguardia dei dati mediante meccanismi di firma e verifica, delle credenziali di sicurezza tutte le fasi, per la consultazione, la scrittura, impostazioni di configurazione e/o l'aggiornamento delle configurazioni.

Un sistema di autorizzazione di componenti M2M tipiche di device IoT deve appartenere ad un processo più ampio che provvede alla gestione degli accessi a risorse e servizi ospitati centralmente.

La procedura di autorizzazione, indipendentemente dal tipo di classificazione sui dati a cui si richiede l'accesso, deve tenere conto che, sia il richiedente che il mittente del messaggio di richiesta di accesso alle risorse, vengano identificati, solo dopo si potrà avere accesso ad una specifica funzione. La medesima attività deve avere riscontro con il ricevente, realizzando in tal modo un'autenticazione reciproca.

Entrambi le risorse devono avere predisposto un meccanismo di controllo (c.d. Access Control Policy) basato su politiche di verifica degli attributi.

Un assunto base della sicurezza riguarda principalmente la salvaguardia delle informazioni che sono considerate il bene più prezioso e importante di una organizzazione.

Nel caso di trattamento di tipologie di dati sensibili (esempio: sanitari) la security deve includere almeno le seguenti funzionalità: chiavi di sicurezza, credenziali locali, politiche di sicurezza, le informazioni sulle identità, informazioni per l'iscrizione e molto altro. Le funzioni sensibili devono includere necessariamente funzioni di crittografia, de-crittografia di dati e firma delle informazioni per garantire il non ripudio che sono la base dei tre assunti sulla sicurezza: riservatezza, integrità e disponibilità.

A supporto della riservatezza e integrità possono essere utilizzate soluzioni specifiche di mercato o realizzate ad-hoc. Ad esempio possono essere implementate Infrastrutture a chiavi pubbliche PKI, in grado di fornire modelli di certificazione delle chiavi pubbliche messe a

disposizione per autenticare e cifrare tali dati ma allo stesso tempo si potranno anche utilizzare soluzioni di mercato ed utilizzare certificati digitali di PKI pubbliche e certificate.

7.4.2. *Standard per la IoT Security*

Se il security by design è l'obiettivo, esso richiederà ancora lo sviluppo delle tecnologie IT appropriate. Per ora la comunità tecnico scientifica ha proceduto a delineare, a volte a completare, gli ambiti di standardizzazione dei temi della security interni alla implementazione dell'Internet of things nei cosiddetti mercati verticali, quali ad esempio: smart home; smart health (comprensivo dei temi della telemedicina, l'assistenza remota e dei dispositivi wearables); smart grid, smart city, smart environment.

Contributi particolari sul tema sicurezza sono da attribuire alla ENISA: *European Union Agency for Network and Information Security* (www.enisa.europa.eu) e alla americana NIST: *National Institute of Standards and Technology* (www.nist.gov).

Trust fra Layer e Piattaforme
ISO/IEC
ISO/IEC 27001, Information technology -- Security techniques -- Information security management systems – Requirements.
ISO/IEC 27039 Detecting and preventing cyber-attacks
ISO/IEC 27017 Protecting information in the cloud
ISO/IEC 31000 Risk Management
NIST National Institute of Standards and Technology
Framework for Cyber-Physical Systems - Draft v.0.8
Trust fra oggetti
ETSI TI M2M WG4
ETSI TS 102 690 Machine-to-Machine communications (M2M) Functional architecture
ETSi TS 102 921 Machine-to-Machine communications (M2M): mIa, dIa and mId interfaces
Crittografia Dati
ENISA - European Union Agency for Network and Information Security
TR Recommended cryptographic measures: Securing personal data
IETF
RFC 4107 Guidelines for Cryptographic Key Management

Tabella 18 - Standard per la IoT Security

E' stato inoltre avviato l'approfondimento, grazie soprattutto al contributo dei Programmi europei per la ricerca, sul tema della sicurezza e della tutela della sicurezza nel mondo dei cyber pysical systems, ovvero dei mondi dove la relazione tra mondo fisico e virtuale appare densa di variabili, non sempre definibili.

In attesa dell'avvento della rete 5G, del deploying massivo della tecnologia cellular like NB-IoT la GSM Association ha pubblicato[36] nel febbraio del 2016 un set di linee guida e raccomandazioni connesse alla implementazione di servizi di telefonia associati all'Internet of Things, ai rischi possibili e alla loro mitigazione.

Reti Mobili
GSM Association
IoT Security Guidelines for Service Ecosystem
IoT Security Guidelines for Endpoints Ecosystem
IoT Security Guidelines for Network Operators

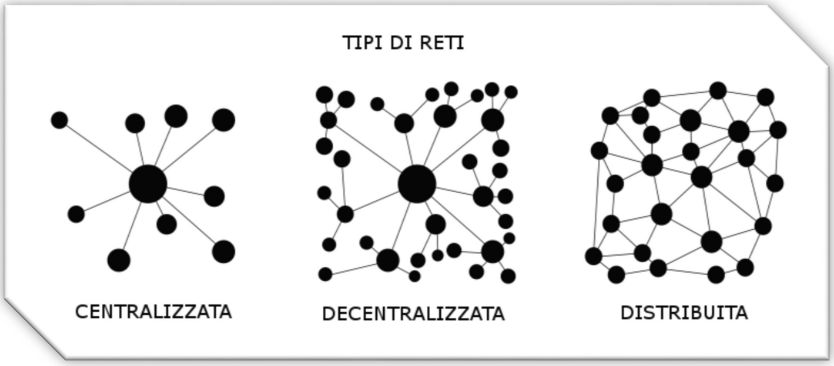
Tabella 19 - GSMA IoT Security Guidelines

Nell'ambito delle best practices di riferimento, oltre quanto proposto nelle tabelle e dai vendor più accreditati, si segnalano i contributi importanti di: OWASP Open Web Application Security Project[37], della Cloud Security Alliance[38] e dello IERC – European Research Cluster on Internet of Things[39].

7.4.3. *IoT Distribuito e Blockchain*

Una delle innovazioni che l'IoT sta portando nel mondo della gestione e controllo di sensori e device è il cambio di paradigma architetturale: si è passati da un modello centralizzato a un modello decentralizzato, dove diversi punti di raccolta (es. smart gateway, fog node) fanno da intermediari tra i dispositivi e servizi centralizzati ad alto valore aggiunto (es. analytics offerti in cloud).

[36] http://www.gsma.com/connectedliving/future-iot-networks/iot-security-guidelines/
[37] https://www.owasp.org/index.php/Main_Page
[38] CSA (2015) Security Guidance for Early Adopter of the Internet of Things
[39] IERC (2015) IoT Governance, Privacy and Security Issue



Benché Internet nasca come rete distribuita di nodi *di pari dignità* (o peer), per ragioni pratiche prima ed economiche poi, lentamente si è trasformata in una rete fortemente centralizzata dove una cerchia ristretta di soggetti monitora, genera ed attira la maggior parte del traffico dati. Con il diffondersi della qualità dei servizi offerti da Internet e il moltiplicarsi degli utenti, i modelli architetturali delle infrastrutture IT si sono dovuti adeguare alle nuove esigenze di performance e scalabilità. Questo ha portato alla creazione di enormi CED sempre più potenti ed evoluti, fino ad arrivare all'attuale modello di CED Cloud.

In tutti questi anni, nonostante le continue spinte economiche e opportunistiche a mantenere ed evolvere questo paradigma fortemente centralizzato, i modelli e le tecnologie P2P (Peer-2-Peer) sono invece lentamente evolute, affermandosi sempre più come alternative valide e a volte indispensabili rispetto ai quelle centralizzate (es. file sharing e messaggistica).

Finora il modello centralizzato ha risposto efficacemente alla vertiginosa crescita del numero di utenti della rete, riuscendo a trasformarsi ed adattarsi nel tempo evolvendo parimenti infrastrutture e tecnologie, relegando essenzialmente la scelta dell'utilizzo di un modello P2P ad una questione di finezze tecnologiche o a considerazioni prettamente funzionali etiche e/o sociali (libertà di espressione, diritto alla privacy, trasparenza e democrazia, ecc.)

È unanime l'idea che l'IoT innalzerà il numero di utenti della rete in maniera esponenziale, introducendo come tali miliardi di dispositivi all'interno della rete. Questo porterà necessariamente a dover considerare un nuovo cambio di paradigma che permetterà di evolvere l'attuale modello IoT decentralizzato – tra l'altro ancora in fase di evoluzione e omogeneizzazione - verso un modello IoT distribuito, sfruttando finalmente appieno la vera natura della rete Internet.

Una delle tecnologie P2P più promettenti dell'attuale panorama IT è la così detta ***Distributed Ledger Technology,*** più comunemente nota come ***Blockchain***[40]***.***

La Blockchain, resa celebre in anni recenti grazie alla diffusione dei Bitcoin, permette di registrare transazioni in modo sicuro e certificato all'interno di singoli blocchi, costantemente concatenati tra loro in ordine cronologico e indissolubile. Il contesto è una rete aperta di peer indipendenti, che possono connettersi autonomamente e scambiare dati tra di loro senza la necessità di contattare alcuna autorità di controllo centrale.

Ai peer non è richiesto alcun atto di fiducia verso un singolo soggetto autoritario: è la rete stessa che tramite algoritmi di consenso condiviso permette o meno che un'informazione venga inviata, memorizzata e mantenuta per sempre integra e valida all'interno del sistema; per questo motivo la rete viene definita Trustless.

Utilizzando la Blockchain, la rete di peer garantisce by design la maggior parte delle condizioni di sicurezza necessarie al mondo IoT. Sistemi più evoluti, come ad esempio la rete **Ethereum**[41]**,** estendono le funzionalità della Blockchain includendo la possibilità di immagazzinare, oltre a dati statici, anche vere e proprie applicazioni all'interno del sistema. In questo modo i programmi diventano per la prima volta veri e propri contratti pubblici ed immutabili - i così detti Smart Contract – ai quali può essere delegata la logica necessaria ed indispensabile affinché un'informazione venga immagazzinata nella Blockchain ed elaborata dai nodi del sistema.

Questa estensione non solo permette un ulteriore ampliamento dei casi d'uso della Blockchain in ambito IoT (e oltre) ma completa la copertura dei requisiti di sicurezza - già citati - che vengono risolti nel momento stesso in cui questa tecnologia viene abbracciata.

[40] https://www.blockchain.com/
[41] https://www.ethereum.org/

Tecnologie utilizzate dalla rete di peer	Confidenzialità	Integrità	Autenticazione	Autorizzazione	Non ripudio	Auditing	Protezione delle Identità
Blockchain	✗	✓	✓	✗	✓	✓	✗
Smart Contract	✓	✗	✗	✓	✗	✗	✓
Blockchain & Smart Contract	✓	✓	✓	✓	✓	✓	✓

Come tutte le tecnologie informatiche, anche la Blockchain si basa su gran parte di codice e tecniche esistenti e consolidate, come la crittografia a chiave asimmetrica utilizzata per la creazione delle utenze e per la firma delle transazioni inviate alla rete, le tecnologie P2P per il discovery dei nodi e la condivisione delle informazioni (es. via protocollo Kademlia), vari algoritmi matematici e strutture dati per l'ottimizzazione delle performance e la garanzia dell'autenticità delle informazioni scambiate (es. Merkle Tree, Directed Acyclic Graph, Distributed Hash Table).

Tutte le tecnologie che circondano il mondo Blockchain e P2P in generale si basano su prodotti open source, ampiamente manutenuti ed evoluti da una fervente community mondiale di developer e pesantemente utilizzate a volte inconsapevolmente dal mondo consumer.

Due elementi sono attualmente da tenere in considerazione durante la progettazione di soluzioni distribuite basate sulla Blockchain: la scarsa scalabilità delle informazioni (i dati sono infatti replicati per intero su tutti i nodi della rete, con conseguente altissima duplicazione delle informazioni ed un consumo di storage sempre crescente) e l'alto consumo energetico, dovuto al meccanismo di consenso distribuito attualmente utilizzato - il così detto Proof of Work - basato sostanzialmente sull'elaborazione di un problema matematico che si fa via via sempre più complesso da risolvere. Per entrambi i punti sono allo studio e alla prova diverse soluzioni. Ci si aspetta che la community sia in grado di risolvere presto o tardi entrambi agevolmente, soprattutto ora che Blockchain e Smart Contract stanno entrando sempre più di prepotenza nei piani di investimento di aziende pubbliche e private.

Per il consumo energetico, in questo momento l'elemento sicuramente più critico e costoso dell'intero sistema, sono già stati realizzati e in fase avanzata di test algoritmi di consenso

alternativi al PoW (es. il Proof-of-Stake) che rimuoverebbero alla radice questa problematica. Per lo storage, si iniziano a diffondere sia soluzioni per immagazzinare le transazioni anche su Blockchain parallele e collegate a quella principale – le così dette Sidechain – sia soluzioni per immagazzinare la maggior parte delle informazioni sulla rete P2P stessa, ed in particolare tramite l'evoluzione degli attuali meccanismi di file sharing tramite Content Addressable Network; sulla Blockchain saranno immagazzinati quindi solamente gli hash identificativi di riferimento dei diversi contenuti, così da avere disponibile contemporaneamente sia l'indirizzo al quale recuperare il contenuto sia garanzia della validità e dell'integrità del contenuto stesso.

7.5. Gli Standard per le Ontologie

Un ruolo essenziale del processi di standardizzazione delle ontologie lo intende assolvere l'iniziativa **oneM2M**, poiché le esistenti applicazioni dell'Internet of Things e del Semantic Web of Things non appaiono interoperabili, in base dei diversi formati, protocolli e definizione dei dati derivanti dai sensori e dei sensori stessi. Per assicurare la interoperabilità delle future applicazioni, oneM2M ritiene infatti essenziale:

- Rendere interoperabili i dati, gli schemi e domini dell'IoT
- Rendere omogenea la classificazione dei dati
- Generare applicazioni che rendano interoperabili i due mondi IoT/SWoT.

Nella figura sono rappresentati gli obiettivi dei processi di standardizzazione di OneM2M Ove, partendo da sinistra, sono indicate le priorità d'azione ai fine della interoperabilità globale: 1) protocolli unici per la comunicazione M2M; 2) comuni protocolli (API) per le comunicazione tra i layer architetturali; 3) comuni ontologie per la astrazione dei sensori e delle misure; 4) creazione della astrazione delle reti: il web of things.

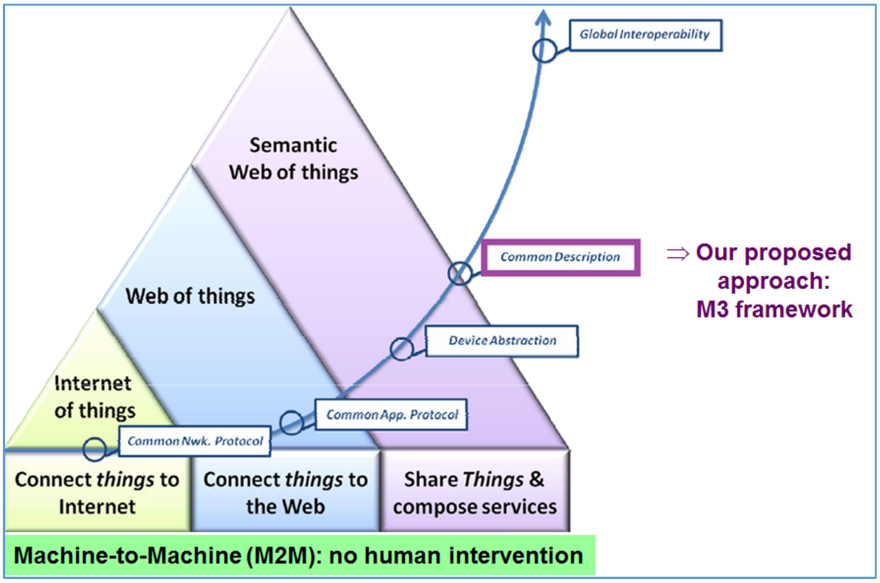


Figura 17 - Processi di standardizzazione delle ontologie secondo oneM2M

La standardizzazione delle ontologie semantiche è elemento chiave per assicurare:

- la interoperabilità;
- la descrizione omogenea delle unità fisiche (device);
- incoraggiare l'uso di un vocabolario comune specialmente rispetto all'uso plurimo dei dati, che le reti del futuro prospettano;
- prevedere una coerenza con linguaggi di modellizzazione in uso nello sviluppo software (esempio: OWL)[42]

Le attività di standardizzazione in corso sul tema sono a carico, oltre cha da oneM2M, dei working groups attivati da: ETSI M2M, W3C SSN ontology e dal W3C WWeb of Things, OGC.

[42] https://www.w3.org/OWL/

Ontologie
oneM2M MAS WG
Input Contribution: A unified language to describe M2M/IoT data
Input Contribution: Semantic Web best practices.
World Wide Web Consortium - W3C SSN-XG Incubator Group
Semantic Sensor Network Ontology
Open Geospatial Consortium OCG
Sensor Web Enablement (SWE)

Tabella 20 - Standard per le ontologie IoT

Lo **IERC** (European Research Cluster on Internet of Things) ha correttamente inserito il tema della analisi semantica all'interno del task della interoperabilità, suddividendo la stessa in segmenti di intervento

- Technical interoperability: tra sistemi hardware e software eterogeni.
- Syntactical interoperability: riguardante il formato dei dati elementari ed aggregati
- Semantic interoperability: relativa alla classificazione / interpretazione del significato dei dati scambiati tra domini o sistemi.
- Organizational interoperability: funzionale alla condivisione dei dati e delle informazioni tra le infrastrutture.

IoT-A è uno progetti di ricerca del 7° Programma Quadro da considerarsi quale pioniere nelle ricerca nel settore dell'Internet of Things. Esso aveva, tra l'altro, sviluppato un toolkit dedicato alla interpretazione dei dati dei sensori, il **Knowledge Acquisition Toolkit (KAT)[43].**

7.6. Esposizione e Uso dei Servizi

Può essere utilizzato lo strumento di *Business Partner Management* per regolare secondo dei Service Level Agreement (SLA) la possibilità di accedere alle API di Piattaforma. Grazie allo strumento di Business Partner Management è possibile realizzare un MarketPlace di Applicazioni, ognuna delle quali caratterizzata da uno specifico agreement. Le Applicazioni

[43] http://kat.ee.surrey.ac.uk/KAT-Manual.html

possono essere esposte agli End Users (Consumers o Enterprise) all'interno di Store multidevice e multipiattaforma, in cui è possibile implementare logiche di e-commerce evolute.

API Management in grado di effettuare throttling, cioè il di controllo del numero di messaggi inviati per unità d tempo, espongono i servizi delle piattaforme di Back End as a Service (le piattaforme del Layer Service e Application) a sistemi verticali, mentre ESB leggeri permettono l'integrazione con i sottosistemi legacy.

I MarketPlace per la ricerca e selezione delle applicazioni sono gli strumenti di fruizione delle soluzioni IoT sia in ambito Industrial sia SmartCommunities, dalle SmartCities alla PA. I meccanismi di attivazione di una soluzione e il loro livello di trasparenza rispetto all'intervento dell'utente o del fornitore di servizio dipende dal modello IaaS e Paas federato sottostante al Marketplace e anche in questo caso alla capacità di interoperabilità dei sistemi MarketPlace, IaaS e Paas (quindi Cloud).

8. Norme sulle sorgenti di campi elettromagnetici

Sul tema delle condizioni per l'utilizzo in sicurezza delle radio frequenze e della influenza dei campi elettromagnetici connessi occorre riferirsi ai contributi metodologici proposti dalla *Organizzazione Mondiale, per la Sanità* ***(World Health Organization - WHO),*** *dall'International Association for Cancer Research* ***(IARC)*** e *dall'International Commission on Non-Ionizing Radiation Protection* ***(ICNIRP)****.*

World Health Organization (WHO)
Environmental Health Criteria 232 Static Fields - 2006
Framework for Developing – Health Based EMF Standards - 2006
Environmental Health Criteria 238 Extremely Low Frequency Fields - 2007
International Association for Cancer Research (IARC)
IARC Non-Ionizing Radiation, Part 1: Static and Extremely Low-Frequency (ELF) Electric and Magnetic Fields - 2002
Commissione Internazionale per la Protezione dalle Radiazioni Non Ionizzanti (ICNIRP)
Linee Guida per la Limitazione dell'esposizione a Campi Elettrici e Magnetici Variabili nel Tempo ed a Campi Elettromagnetici (Fino a 300 Ghz) - 1998

Tabella 21 Campi elettromagnetici: linee guida sugli effetti e sui limiti alla esposizione

I limiti attualmente in vigore in Italia sono stati fissati dal ***Decreto del Presidente del Consiglio dei Ministri dell'8 luglio 2003 (Gazzetta Ufficiale n. 199 del 28/08/2003)***[44] emanato ai fini della protezione della popolazione dalle esposizioni a campi elettrici, magnetici ed elettromagnetici generati da sorgenti fisse operanti ad alta frequenza, comprendenti, ad esempio, gli impianti per telefonia mobile o per radiodiffusione televisiva o radiofonica. In esso vengono fissati nell'ordine limiti di esposizione, valori di attenzione ed obiettivi di qualità:

- Limite di esposizione: si intende il valore di campo elettrico, magnetico ed elettromagnetico, considerato come valore di immissione, definito ai fini della tutela della salute da effetti acuti, che non deve essere superato in alcuna condizione di esposizione della popolazione […].
- Valore di attenzione: si intende il valore di campo elettrico, magnetico ed elettromagnetico, considerato come valore di immissione, che non deve essere superato negli ambienti abitativi, scolastici e nei luoghi adibiti a permanenze prolungate […] Esso costituisce misura di cautela ai fini della protezione da possibili effetti a lungo termine […].
- Obiettivi di qualità: si intendono i valori di campo elettrico, magnetico ed elettromagnetico, definiti dallo Stato […], ai fini della progressiva minimizzazione dell'esposizione ai campi medesimi.

Le limitazioni attualmente in vigore in Italia risultano essere più restrittive di quanto raccomandato dall'ICNIRP (accolto dell'Unione Europea e da molti altri Stati) e di quanto previsto dalle norme statunitensi. Infatti, l'Italia ha adottato un approccio normativo cautelativo nei confronti di eventuali effetti a lungo termine conseguenti ad esposizioni prolungate nel tempo e a bassi livelli di campo. In particolare, nella regione compresa tra 400 MHz e 3 GHz i limiti di esposizione sono pari a 1/3 degli standard europei e statunitensi.

[44] Fissazione dei limiti di esposizione, dei valori di attenzione e degli obiettivi di qualità per la protezione della popolazione dalle esposizioni a campi elettrici, magnetici ed elettromagnetici generati a frequenze comprese tra 100 kHz e 300 GHz.

Limiti di Esposizione		
(f=frequenza)	Intensità campo elettrico	Intensità campo magnetico
	E (V/m)	H (A/m)
0,1 < f ≤ 3 MHz	60	0,2
3 < f ≤ 3000 MHz	20	0,05
3 < f ≤ 300 GHz	40	0,10
Valori di attenzione Intensità di Intensità di e obiettivi campo elettrico campo magnetico di qualità		
Limiti di Esposizione	Intensità campo elettrico	Intensità campo magnetico
(f=frequenza)	E (V/m)	H (A/m)
0,1MHz< f ≤ 300GHz	6	0,016

Relativamente agli standard tecnici delle linee, apparati, strumenti e sistemi emittenti campi elettromagnetici occorre riferirsi ai contributi tecnici sviluppati dagli International Committee on Electromagnetic Safety in collaborazione con l'Institute of Electrical and Electronic Engineers (IEEE/ICES); dall'International Electrotechnical Commission (IEC), dall' European Committee for Electrotechnical Standardization (CENELEC), così come dai diversi enti di standardizzazione nazionali. Il Contributo dello IEEE/ICES è utilizzato quale comune riferimento.

Institute of Electrical and Electronic Engineers (IEEE)
IEEE Std C95 1 - 2005 - IEEE Standard for Safety Levels with Respect to Human Exposure to Radio Frequency Electromagnetic Fields, 3 kHz to 300 GHz
IEEE Std C95 1.a - 2010 Amendment 1. Specific Ceiling Limits for Induced and Contact Current Classifies Distribution beteween Localized Exposure and Spatial Peak Power Density
IEEE Std C95 3.1 - 2010 Recomendated Practices for Measurement and Computatuon od electric, magnetic, Electromagnetic Fields with Respect to Human Exprosure to Such Filed 0 Hz to 100 kHz
IEEE Std C95 7 - 2014 IEEE Recomendated Practice for Radio Frequency Safety Programs 3 kHz Ghz
IEEE Std C95.1-2345 -2014 IEEE Standard for Military Workplaces—Force Health Protection Regarding Personnel Exposure to Electric, Magnetic, and Electromagnetic Fields, 0 Hz to 300 GHz

Tabella 22 IEEE Standard tecnici per la esposizione e la misura dei campi elettromagnetici

9. Servizi Cloud per l'IoT

Ogni impresa che intende avviare un progetto di implementazione di soluzioni di internet of things deve porsi quesiti importanti, le cui risposte potrebbero orientare il modello stesso di introduzione delle nuove tecnologie nei suoi processi di business. L'adozione di architetture e servizi **Cloud Based è** un passo necessario per ridurre drasticamente la complessità delle architetture tecnologiche immaginate, i costi dello sviluppo, di implementazione, gestione delle reti e dei sistemi, nonché del loro continuo aggiornamento.

Nella scelta delle opzione Cloud occorre considerare anche altri requisiti importanti.

La Scalabilità. Nella realizzazione di un Sistema IoT occorre considerare la tipologia, numerosità, localizzazione dei sensori, attuatori, device che dovranno essere collegati. La tipologia di connessioni che saranno utilizzate, le necessità di elaborazione e condivisione dei dati. In sistemi altamente distribuiti le funzionalità richiedenti elaborazioni ed azioni real time dovranno essere presidiate con logiche e soluzioni specifiche.

I Big Data & Analytics. I sistemi IoT più avanzati, ovvero tutti i sistemi IoT nel tempo, produrranno una vasta quantità di dati. L'abilità di analizzare le serie storiche come i dati puntuali per ricavarne informazioni utili sia alla gestione ordinaria dei servizi sia allo sviluppo del business sarà una caratteristica essenziale del valore offerto dal sistema IoT. Sarà necessario disporre di soluzioni dedicate alla elaborazione dei dati.

L' eterogeneità dei sistemi. I sistemi IoT saranno spesso costruiti su substrati tecnologici esistenti, aggiornati per estenderne le funzionalità con sistemi nativamente IoT. Linguaggi, protocolli, connessioni altamente diversi richiederanno moduli ad hoc per la interoperabilità, incrementando la complessità.

La Sicurezza e la Privacy. Il tema della sicurezza in sistemi altamente distribuiti, scalabili, in rapida continua evoluzione non è affrontabile con la classica interposizione stand alone di soluzioni, anche le più performanti. La chiave del successo è il continuo, sempre più avanzato, monitoraggio dei servizi, l'aggiornamento continuo delle applicazioni e delle protezioni a tutti i livelli della infrastruttura.

Le Competenze. I diversi settori tecnologici impattati impongono di poter disporre di competenze e di skill professionali altamente specialistici, anche se per periodi di tempo limitati.

La Velocità. Elemento chiave della competitività di ogni azienda nei propri mercati è dato dalla velocità con cui si attuano i cambiamenti, si arriva prima sui mercati, si erogano servizi. La velocità di implementazione è garantita dall'accesso a modelli di servizio cloud ampiamente sperimentati (Paas, Iaas, Saas) e modelli di deploying estremamente flessibili (privato, pubblico, ibrido).

Il mercato offre tutti i componenti necessari per creare efficienti sistemi M2M distribuiti, servizi cloud nei quali migliaia di dispositivi e sensori sono in grado di dialogare e collaborare tra loro, con le business application e le infrastrutture IT residenti nei data center on premise o nel cloud.

I componenti della architetture Cloud IoT sono inseribili in una architettura 3-tier comprendente: Edge, IoT ed Enterprise Tiers.

- L'Edge comprende il Proximity Network e il Public Network dove i devices sono collegati direttamente o tramite gateway, dotati di maggiori o minori risorse computazionali.
- IoT Platform Tier è offerto dal provider dei servizi cloud IoT. Riceve, processa e analizza i dati provenienti dall'Edge level, offre ambienti di API management e di visualizzazione. Permette il controllo e la gestione remota dei device (sensori, attuatori)
- L'Enterprise Tier comprende sia tutti i tipici servizi gestionali e applicativi di interesse (Enterprise Data, Enterprise User Directory, Enterprise Applications) sia i servizi verticali di accesso o di sicurezza.

Sono già attive le piattaforme cloud che possono ridurre il time-to-market e che permettono di realizzare progetti scalabili ed efficienti.

Forrester Research[45] ha proposto una analisi dei best vendor sulla base di diversi indicatori tecnici e di servizio. Nella figura sono rappresentati i ruoli assunti sul mercato.

[45] Forrester: The Forrester Wave (2016) IoT Software Platform Q4

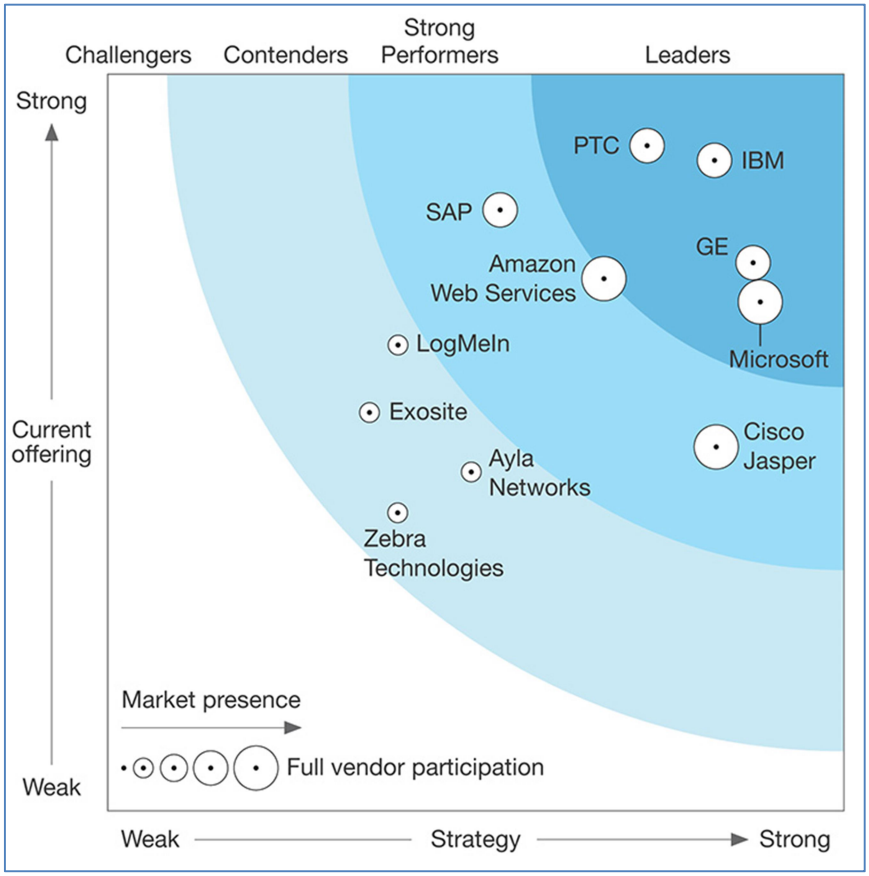


Figura 18 – Forrester Cloud IoT Leader Quadrant

Un primo elenco di servizi disponibili è proposto nella tabella

Denominazione	Link
AWS (Amazon Web Services) IoT	https://aws.amazon.com/it/iot-platform/how-it-works/
Cisco IoT Cloud Connect	http://www.cisco.com/c/en/us/solutions/service-provider/iot-cloud-connect/index.html
Eurotech	https://www.eurotech.com/it/prodotti/software+m2m
General Electric Predix	https://www.ge.com/digital/predix
IBM Watson Internet of Things	http://www.ibm.com/internet-of-things/
iNebula	https://www.inebula.it/
Microsoft Azure IoT	http://www.microsoft.com/it-it/server-cloud/internet-of-things/azure-iot-suite.aspx
Orade IoT	https://cloud.orade.com/iot
PTC Thingsworx	http://www.ptc.com/internet-of-things/technology-platform-thingworx
Salesforce Cloud IoT Einstein	http://www.salesforce.com/iot-cloud/
Sap Hana Cloud Platform	https://hcp.sap.com/capabilities/iot.html

Tabella 23 IoT Cloud Services Vendor

10. L'internet of things nella società digitale

L' internet of things (IoT) è un fenomeno che si sta velocemente affermando come paradigma rivoluzionario nello scenario delle nuove telecomunicazioni senza fili. L'idea alla base di questo concetto è la pervasiva presenza di una gran quantità di cose o oggetti che attraverso varie tecnologie abilitanti sono in grado di interagire tra di loro e co-operare per il raggiungimento di un obiettivo comune. L'internet delle cose è la rete di oggetti fisici che dispongono intrinsecamente della tecnologia necessaria per rilevare e trasmettere informazioni sul proprio stato o sull'ambiente esterno. L'IoT è composto da un ecosistema che include le cose, gli apparati necessari per garantire le comunicazioni, le applicazioni e i sistemi per l'analisi dei dati. Secondo gli analisti entro il 2020 ci saranno più di ventiquattro miliardi di dispositivi connessi, che approssimativamente corrispondono a quattro devices per ogni essere umano sulla terra. Inoltre secondo l'americana Cisco entro il 2020 il valore aggiunto complessivo all'economia globale sarà di 14.000 miliardi di dollari. È fuori dubbio, quindi, che le potenzialità derivanti da un'applicazione completa di questo paradigma portino sia ad una rivoluzione industriale sia ad un radicale cambiamento di molti aspetti della vita quotidiana e comportamentale delle persone. Dal punto di vista di un utente privato, gli effetti più ovvi dell'introduzione dell'internet of things saranno visibili sia dal lato lavorativo che domestico. In questo contesto la domotica, l'assistenza virtuale, l'e-health sono solo alcuni esempi dei possibili scenari in cui questo nuovo paradigma rappresenterà un ruolo chiave nel futuro prossimo. Dal punto di vista degli utenti business, le conseguenze più evidenti saranno in campi come quello dell'automazione e dell'industria manifatturiera o relativi al business/process management ed al trasporto intelligente di risorse. Inoltre la grande mole di dati prodotti dai dispositivi connessi apriranno nuovi scenari per nuovi modelli di business basati sulla gestione e valorizzazione dei dati condivisibili.

10.1. Gestione e analisi dei big data

L'importanza dei dati e della loro analisi e condivisione è ormai oggetto di tanti studi di merito. La Gartner company definisce l'informazione come il petrolio del ventunesimo secolo sottolineando come un dato strutturato possa generare un valore che innesca nuovi scenari di business e value creation. Nel paradigma IoT, un'enorme quantità di sensori sono collegati a dispositivi e macchine del mondo reale. I sensori hanno la capacità di collezionare vari tipi di dati come ad esempio informazioni sull'ambiente, sull'astronomia, sulla logistica o sulla salute del paziente. I big data prodotti dall'IoT hanno caratteristiche differenti rispetto ai classici big data a causa delle diverse tipologie di dati collezionabili i quali sono eterogenei, vari, destrutturati, disturbati e ad alta ridondanza. Entro il 2030 la quantità di sensori raggiungerà le 3 miliardi di unità e quindi i dati prodotti dall'IoT rappresenteranno la componente principale di tutti i big data. Risulta quindi di fondamentale importanza superare l'attuale situazione in cui l'IoT è un semplice collezionatore di dati per passare all'introduzione di tecnologie che promuovano lo sviluppo dell'analisi dei big data.
I dati generati dell'internet of things presentano le seguenti caratteristiche :

- Large-scale data: i dati raccolti in ambito IoT possono essere semplici dati numerici, come la localizzazione, oppure complessi dati multimediali, come un video di sorveglianza. Per affrontare le richieste di analisi, non sono registrati solo i dati correnti bensì anche quelli storici in un determinato periodo di tempo;
- Heterogeneity: data la varietà dei dispositivi che acquisiscono i dati, le informazioni prodotte sono tutte differenti ed eterogenee;
- Strong time and space correlation: nell'IoT ogni dispositivo che genera dati è posizionato in uno specifico spazio geografico ed ogni pezzo di dato prodotto ha un proprio "time stamp". Durante l'analisi e l'elaborazione dei dati, il tempo e lo spazio risultando dimensioni fondamentali per le analisi statistiche;
- Effective data accounts for only a small portion of the big data: durante l'acquisizione e la trasmissione dei dati nell'IoT, potrebbero verificarsi una grande quantità di disturbi o deviazioni. Quindi tra tutti i dati collezionati, solo una piccola parte sarà suscettibile di valutazione. Ad esempio durante l'acquisizione dei video di sorveglianza del traffico,

saranno importanti e di valore i soli frame che riprendono l'eventuale effrazione e non tutto il resto del video raffigurante la normale congestione del traffico;

L'internet of things non è solo un'importante fonte di creazione di big data, ma è anche il principale mercato per le applicazioni dei big data. A causa dell'alta varietà di oggetti e sensori, le applicazioni in questo settore sembrano evolversi all'infinito. Ad esempio le imprese di logistica sono state tra le prime a trarre significativi vantaggi dallo sfruttamento dei big data prodotti dall'IoT. I camion dell'UPS sono equipaggiati con sensori wireless GPS così che il quartier generale possa sia tracciare la posizione del mezzo sia prevenire eventuali guasti meccanici. Inoltre il sistema supporta gli impiegati autisti dei camion attraverso l'ottimizzazione delle rotte per le consegne. Il tragitto ottimale, infatti, deriva dalle passate esperienze accumulate. Nel 2011 gli autisti UPS hanno guidato risparmiando un ammontare di circa 48 milioni di chilometri.

10.2. Settori di applicabilità

Le potenzialità offerte dall'internet of things riguardano un grande numero di applicazioni, delle quali solo una piccola parte sono attualmente disponibili. Sono tanti i settori e gli ambienti nei quali queste nuove applicazioni miglioreranno la qualità delle nostre vite: a casa, in viaggio, a lavoro, in palestra, solo per citarne alcune. Se gli oggetti utilizzati per compiere azioni quotidiane si trasformano in oggetti smart in grado di elaborare e condividere informazioni, i cambiamenti saranno radicali e nuovi scenari si apriranno. Dividiamo le possibili applicazioni nei seguenti quattro gruppi: Industry 4.0, Smart health, Smart environment, personal and social domain.

10.2.1. *Industry 4.0*

Il termine industria 4.0 indica una tendenza dell'automazione industriale che integra nuove tecnologie produttive per migliorare le condizioni di lavoro ed aumentare la produttività e la qualità produttiva degli impianti. La chiave di volta dell'industry 4.0 è la decentralizzazione e la collaborazione tra i sistemi che avviene tramite il collegamento dei sistemi fisici con i sistemi

informatici. L'interazione e la collaborazione tra questi due sistemi rappresenta un'innovazione strutturale che cambia radicalmente i processi produttivi e gestionali. Il termine fu coniato per la prima volta dalla Germania, che nel 2011 presentò un piano industriale per il rilancio del sistema produttivo tedesco a livello globale. L'impatto di queste nuove politiche sono state successivamente oggetto di approfonditi studi da parte dei più grandi osservatori mondiali, i quali hanno definito questo passaggio storico "Quarta rivoluzione industriale" per l'impatto che avrà sul contesto sociale ed economico. In un recente studio del Boston Consulting group, vengono elencate le tecnologie abilitanti per l'adozione di politiche di industry 4.0.
Esse sono:

- Advanced manufacturing solution: sistemi avanzati di produzione interconnessi e modulari (robotica collaborativa avanzata) ;
- Additive manufacturing: sistemi di produzione additiva che aumentano l'efficienza dell'uso dei materiali ;
- Augmented reality: sistemi di visione con realtà aumentata ;
- Simulation: simulazione tra macchine interconnesse per ottimizzare i processi ;
- Horizontal e vertical integration: scambio di informazioni orizzontale o verticale per potenziare il processo priduttivo ;
- Industrial internet: comunicazione tra elementi della produzione, esterni od interni;
- Cloud: implementazione di tecnologie cloud computing per l'immagazzinamento e l'analisi delle informazioni ;
- Cyber security: tematica della sicurezza delle informazioni e dei sistemi informatici ;
- Big Data Analytics: previsioni o predizioni derivanti dall'analisi strutturale di grandissime quantità di dati .

Tutte queste tecnologie abilitanti sono collegate in maniera diretta o indiretta al paradigma dell'internet delle cose. Senza la creazione di un ecosistema formato da network di dispositivi interconnessi, non potrebbe esserci la condivisione e quindi l'analisi dei dati prodotti, che

risulta fondamentale per il raggiungimento di obiettivi efficienti propri dell'industry 4.0. Nello specifico, i benefici attesi dall'applicazione dell'IoT all'industria sono:

- Integrare virtualmente la Supply Chain e le filiere, garantendo risposte immediate alla volatilità della domanda ;
- Migliorare la qualità dei prodotti con precise informazioni raccolte sull'impianto in tempo reale;
- Risparmiare su spese operative ed energetiche grazie a gestione e controlli remoti; Minimizzare i tempi di inattività degli impianti grazie a strategie di manutenzione predittiva; Incrementare la produttività del lavoro per mezzo del tracciamento di persone e strumenti ;
- Avviare nuovi modelli di business resi possibili dalla connettività in tempo reale con gli impianti industriali.

Il trasporto e la logistica sono altri elementi che subiranno notevoli cambiamenti sia a livello business, e quindi industriale, che a livello consumer, e quindi di vita quotidiana. Le tecnologie basate sui sensori RFID e NFC possono generare informazioni real-time per il monitoraggio contestuale di qualsiasi dispositivo collegato alla filiera produttiva, dall'approvvigionamento delle materie prime ed il loro immagazzinamento, alla distribuzione ed ai processi post-vendita. L'impresa può così rispondere in maniera tempestiva a cambiamenti repentini del mercato. Wal-Mart e Metro, ad esempio, attraverso l'utilizzo di queste tecnologie riescono a ridurre ad un paio di giorni i tempi di risposta ai cambiamenti del mercato, lavorando con un magazzino sostanzialmente vuoto. Inoltre dal punto di vista del consumatore una gestione real-time del magazzino può aiutare i venditori ad assistere meglio il consumatore, informandolo sulla precisa disponibilità di un prodotto. Infine, attraverso dei pannelli interattivi, l'utente potrebbe ricevere informazioni dettagliate riguardo una serie di categorie e ad esempio acquistare un determinato prodotto o servizio semplicemente puntando il proprio dispositivo mobile. La questione della tracciabilità del prodotto o del servizio apre nuovi scenari in cui l'internet of things potrebbe essere utilizzato per regolare le questioni di appropriabilità dell'innovazione.

10.2.2. *Smart Health*

I benefici apportati dalle tecnologie IoT al dominio della sanità sono molti e possono essere raggruppati in quattro categorie:

- Tracking di oggetti e persone (staff e pazienti): il tracciamento è l'identificazione di persone o oggetti in movimento. Esso include sia il monitoraggio real-time di pazienti, per migliorare il flusso di lavoro negli ospedali, sia la localizzazione dei movimenti presso i punti di congestionamento, per gestire l'accesso a determinate aree. Per quanto riguarda gli asset, la localizzazione è applicata agli oggetti dell'inventario ospedaliero, ad esempio per definirne la disponibilità o l'usura.
- Identificazione e autenticazione delle persone: l'identificazione dei pazienti riduce incidenti dannosi come il sovraddosaggio o l'errata somministrazione di farmaci e permette la registrazione di tutte le cartelle mediche digitali del paziente nonché di tutte le nascite per evitare il mismatching dei neonati. Per quanto riguarda gli asset, l'autenticazione di tutto l'inventario permette di rispettare le procedure di sicurezza ed evitare furti o perdite di importanti strumenti;
- Raccolta di dati: immagazzinare e trasferire automaticamente le informazioni riduce i tempi di processo dei moduli ospedalieri, permette l'automazione dei processi di revisione nonché una perfetta gestione dell'inventario medico;
- Sensing: i dispositivi per la rilevazione attivano funzioni centrate per il paziente ed in particolare per diagnosticare le condizioni del paziente attraverso informazioni real-time sugli indicatori di salute critici. Diversi sistemi di monitoraggio dei bio-segnali del paziente a distanza possono essere utilizzati per raggiungerlo ovunque, intervenendo a distanza in caso di complicazioni con precise prescrizioni mediche.

10.2.3. *Smart environment*

Uno dei settori di applicabilità più interessanti dell'internet delle cose è lo smart environment, cioè la trasformazione degli ambienti in sistemi intelligenti composti da dispositivi autonomi ed interconnessi. Oggetti dotati di sensori distribuiti in casa o in ufficio possono rendere la vita più confortevole sotto diversi punti di vista: l'impianto di riscaldamento potrebbe essere adattato alle nostre preferenze o alle condizioni climatiche esterne; l'illuminazione potrebbe automaticamente regolarsi in base alle nostre esigenze o all'orario del giorno; gli incidenti domestici potrebbero essere evitati con appropriati sistemi di allarme; gli sprechi di elettricità potrebbero essere evitati spegnendo i dispositivi quando non usati. Il concetto di città intelligente, o smart city, è l'estremizzazione dei principi dell'internet of things applicati all'innovazione urbanistica. Sfruttando le nuove tecnologie di telecomunicazione, l'intento è quello di migliorare i servizi pubblici mettendo in relazione le infrastrutture materiali delle città con il capitale umano, intellettuale e sociale di chi le abita. Le smart cities sono una risposta alle crescenti sfide affrontate dalle città di oggi, per combinare obiettivi quali lo sviluppo socio-economico e la qualità della vita. Il servizio per eccellenza che gode di significativi benefici derivanti dall'applicazione di tecnologie IoT, è il trasporto pubblico. Macchine, treni e autobus, insieme alle strade o alle rotaie, dotati di sensori e potenti processori, forniscono importanti informazioni agli autisti o ai passeggeri per migliorare la navigazione e la sicurezza. I sistemi di prevenzione delle collisioni ed il monitoraggio del trasporto di materiali pericolosi sono due tipici esempi di possibili funzionalità. Le autorità governative trarrebbero beneficio dalle accurate informazioni circa il traffico per intenti di pianificazione strategica. Il trasporto privato o le imprese, invece, sarebbero preventivamente avvisati di eventuali incidenti o situazioni di traffico e potrebbero così pianificare meglio le rotte ottimali per risparmiare tempo e risorse.

Le palestre e i musei sono altri esempi rappresentativi di come l'applicazione di tecnologie IoT può migliorare la fruizione dei servizi da parte degli utenti. Nei musei le esposizioni potrebbero evocare diversi periodi storici adattando le varie condizioni climatiche. La struttura terrebbe conto delle condizioni esterne ed interne per offrire un'esperienza realistica al visitatore. In palestra, invece, il personal trainer potrebbe caricare la scheda profilo del cliente direttamente all'interno dell'attrezzo, che automaticamente riconoscerebbe l'utente attraverso un tag RFID e personalizzerebbe gli esercizi in base ai parametri vitali registrati. Un'applicazione futuristica nell'ambito delle smart cities, è l'idea del City Information Model (CIM). Il CIM è basato su un concetto che lo stato e la performance di ogni infrastruttura o componente urbana (come i

marciapiedi, i percorsi per i ciclisti o per gli autobus) sono costantemente monitorati dalle autorità della città e le informazioni sono rese disponibili a terze parti, anche se confidenziali. Di conseguenza, niente può essere costruito legalmente se non è compatibile con il CIM. I servizi pubblici comunicherebbero tra di loro i vari consumi di risorse, automaticamente compenserebbero dei surplus ed i prezzi sarebbero calcolati precisamente per allineare domanda e offerta.

10.2.4. *Personal and social domain*

Le applicazioni dell'IoT in questo ambito sono quelle che permettono agli utenti di interagire con altre persone per mantenere e costruire relazioni sociali. I social network sono un esempio lampante di come utilizzare l'aggiornamento automatico delle informazioni personali e condividerle sui portali social. Sensori RFID posizionati su dispositivi di utilizzo quotidiano potrebbero automaticamente condividere sul network le informazioni generate dall'utente, come foto, video o abitudini di consumo, così da generare dei feeback utili per gli altri utenti della rete. I dati storici raccolti dai dispositivi utilizzati, potrebbero essere immagazzinati e classificati per creare una sorta di diario digitale. L'interrogazione di questo diario da parte dell'utente darebbe come risultati tutte le esperienze pregresse e tutti i trend storici di comportamento, utili per una programmazione migliore della vita. Infine gli oggetti dotati di opportuni sensori, potrebbero prevenire furti o smarrimenti semplicemente indicando all'utente la propria posizione o lo spostamento non autorizzato.

11. IoT in ambito sanitario - Ospedale 4.0

L'Ospedale 4.0 introduce un nuovo modo di concepire l'ospedale dove l'architettura, il processo di consegna delle cure sanitarie, l'assistenza sanitaria, il monitoraggio medico, le sale di attesa e gli orari cambiano radicalmente per adattarsi e servire con successo pazienti e medici. Il contesto ospedaliero ormai è un flusso continuo di persone e di dati, dove sempre più discipline operano per personalizzare le soluzioni di cura. I pazienti saranno in grado di

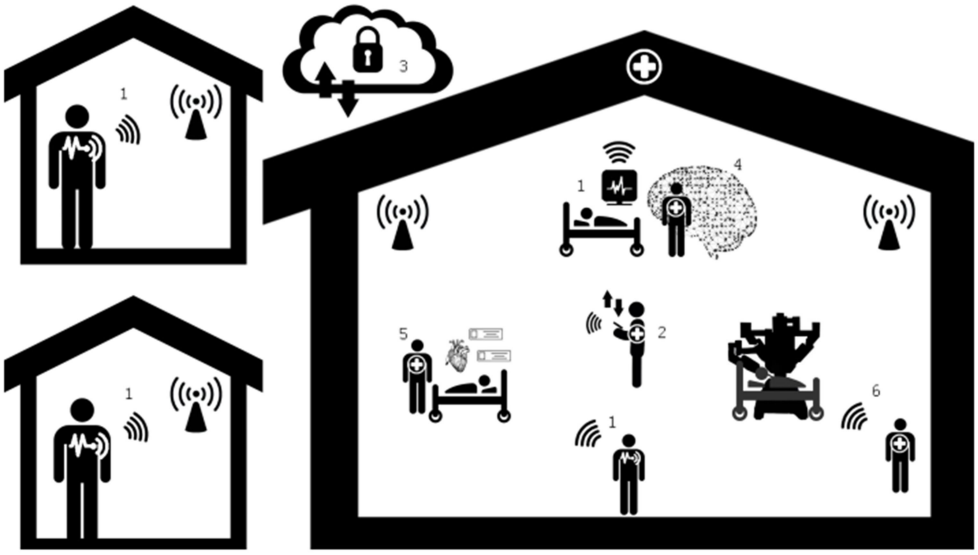
scaricare i propri dati sanitari dai vari dispositivi indossabili e sensori anche prima di consultare il medico, le loro cartelle cliniche e gli archivi saranno digitalizzati e tutte queste informazioni saranno salvate nel cloud in maniera sicura ed efficiente . L'ospedale viene visto non più come edificio", ma piuttosto come "insieme di processi e tecnologie" che dall'edificio si diramano pervadendolo sul territorio diventando una sorta di fulcro, dove vi convergono diverse discipline, tecnologie di ogni genere e flussi di dati provenienti da una intricata rete di processi e relazioni. L'edificio rimarrà preposto alle unità di emergenza e alle sale operatorie, mentre l'assistenza sarà spostata in un ambiente domestico. Questo tipo di assistenza domiciliare offre un servizio di controllo e supporto remoto ai pazienti che soffrono di patologie croniche o che sono in fase postoperatoria o, più semplicemente, prevenzione di determinate patologie tramite sensori biomedici e una connessione costante a un medico.
Questa nuova tipologia di ospedale `e un posto modellato a partire da quattro fattori :

- esigenze del paziente;
- esigenze lavorative del personale medico;
- tecnologia;
- processi di produzione ed erogazione delle prestazioni sanitarie, cliniche chirurgiche.

Inoltre sarà il luogo dove migliaia di dispositivi sono collegati in rete e comunicano tra di loro: dai sensori ai dispositivi medici, dagli apparati più o meno complessi legati alla diagnostica alle attrezzature in sala operatoria, sino ad arrivare in reparto e a bordo letto del paziente.
L'Ospedale 4.0 potrà beneficiare delle tendenze tecnologiche attuali come: occhiali per realtà aumentata, proiezioni di immagini in realtà virtuale, stampanti 3D, computer cognitivi o robot medici che possono rendere le cure meno costose e più efficienti. I vari dispositivi e sensori comunicheranno via wireless con altri dispositivi dove i dati rilevati verranno inviati alla sede fisica dell'ospedale e utilizzati dal personale addetto che si occuperà delle diagnosi e terapie da remoto. Tecniche di cognitive computing organizzeranno la logistica minimizzando i tempi di attesa o dirigeranno le varie persone sul dove e sul quando andare analizzando semplicemente la loro documentazione. Sarà il posto dove la medicina, l'informatica, l'ingegneria clinica, il

design e l'architettura ospedaliera trovano finalmente un punto di incontro. Da parte di chi progetta queste soluzioni tecniche vi è richiesta massima attenzione riguardo la sostenibilità delle soluzioni, la sicurezza e le modalità di comunicazione.

Di seguito si riportata uno schema dell'Ospedale 4.0.



Punto 1 monitoraggio tramite sensori; punto 2 accesso remoto da parte del personale medico ai dati medici; punto 3 tecniche di cloud computing per l'archiviazione dei dati; punto 4 intelligenza artificiale a supporto del processo decisionale; punto 5 realtà aumentata; punto 6 ausilio di robot in ambito chirurgico.

11.1. Pervasive Computing & Internet of Things

Le tecnologie mobili, pervasive e onnipresenti offrono soluzioni promettenti per documentare i progressi, diagnosticare le condizioni e trattare e gestire le cure del paziente con un approccio incentrato su di esso. Inoltre i progressi nel campo delle tecnologie indossabili e delle reti wireless composte da sensori stanno aprendo la strada per la nuova definizione di ospedale e sanità: passando dalla telemedicina all'integrazione di tecnologie mediche specializzate già esistenti con tecnologie pervasive.

Diverse sono le innovazioni fornite da questi sistemi di nuova generazione :

1. sviluppo di funzionalità di monitoraggio continuo per il paziente;

2. miglioramento dei flussi di lavoro e della produttività del personale medico nelle strutture;

3. maggiore connettività consentendo la comunicazione e lo scambio di dati ai pazienti, ai medici e agli operatori sanitari, ovunque e in qualsiasi momento, assegnando così alle comunicazioni pervasive un ruolo fondamentale nel sistema ospedaliero.

I principali domini applicativi di questa integrazione possono essere: il monitoraggio remoto del paziente, l'assistenza, in particolare quella per anziani, gli interventi di emergenza, l'ottimizzazione del flusso di lavoro e la localizzazione degli strumenti. I tradizionali sistemi informativi basati su desktop non sono efficaci dato che il lavoro clinico degli operatori sanitari richiede una stretta collaborazione tra specialisti distribuiti nello spazio e nel tempo dato che la maggior parte dei medici ha bisogno di spostarsi continuamente in strutture ospedaliere per accedere a persone, conoscenze e risorse. Da ciò si può notare come le informazioni sono distribuite in luoghi diversi e non concentrate in un singolo luogo. Di conseguenza, l'ospedale si può considerare come uno spazio di informazioni ampio e complesso dove i medici devono navigare efficacemente per svolgere il proprio lavoro.
La sfida per il passaggio a un Ospedale 4.0 sta nel supporto di medici altamente mobili con ambienti di elaborazione pervasivi, sistemi di informazioni sensibili al contesto, sistemi di archiviazione e note e sistemi per la coordinazione e la collaborazione del personale medico. L'intero sistema pervasivo fornirà ai medici l'accesso alle informazioni che stanno cercando da qualsiasi punto all'interno dell'ospedale attraverso una varietà di dispositivi eterogenei.
Data la sua natura ubiquitaria, l'Internet of Things, è la tecnologia più indicata per poter gestire e monitorare tutte le entità del sistema sanitario offrendo un approccio ben strutturato e di qualità per migliorare la salute e il benessere dei pazienti.

Si prevede che i sistemi basati su questa tecnologia possano rimodellare il settore sanitario in termini di benefici sociali e di costi, come l'applicazione di queste tecnologie all'assistenza sanitaria. Così facendo è possibile migliorarne sia la qualità che i costi automatizzando le attività precedentemente svolte da personale umano. Per creare un ecosistema completo, l'IoT, ha bisogno di essere integrato con i servizi cloud dove i sensori di una rete possono sincronizzare i dati in modo trasparente attraverso l'infrastruttura IoT. Questi dati generati dai sensori collegati ai pazienti sono messi a disposizione di operatori sanitari, familiari e altri utenti autorizzati che danno loro la possibilità di controllare le varie statistiche vitali del soggetto da qualsiasi luogo e in qualsiasi momento. Va notato però che il cambio di paradigma verso sistemi sanitari onnipresenti genera nuove sfide causate dal soddisfare requisiti di Sicurezza e Privacy.

11.2. Sensoristica

Opportunità importanti per l'IoT in ambito sanitario sono il monitoraggio e l'assistenza a distanza, grazie a tecnologie e protocolli per la comunicazione wireless come il Wi-Fi, Bluetooth, NFC, ZeegBee eccetera che sono entrati nell'uso comune. Le caratteristiche tecniche dei vari dispositivi per il rilevamento di parametri vitali si sono evolute talmente velocemente da aver ridotto le proprie dimensioni e migliorato la propria efficienza energetica, per cui questi dispositivi sono diventati sempre più performanti e utilizzabili in contesti diversi. Il monitoraggio viene permesso dalle reti corporee, dette anche Body Area Network, che sono la combinazione dei dispositivi wireless con i vari sensori che prelevano dati fisiologici. I dispositivi fungono da gateway che raccolgono i dati provenienti dai sensori e poi, in un secondo momento, li trasmetterà al back-end della rete che li memorizza per un futuro utilizzo. I dati possono essere salvati con tecniche che ne garantiscono la privacy in server medici nazionali tramite tecnologia cloud e analizzati in seguito con tecniche di analisi dei big data]. I vari sensori, per il monitoraggio a distanza e non, possono essere impiegati per il prelievo di informazioni sul sangue, battiti cardiaci, temperatura corporea e molto altro.

Vi è una classificazione dei sensori utilizzati per l'acquisizione di dati corporei:

- Impiantabili: richiedono una procedura ospedaliera per impiantarli all'interno del corpo del paziente;
- Minimamente invasivi: richiedono la penetrazione della pelle del paziente per funzionare correttamente;
- Non invasivi: richiedono solo l'applicazione sovracutanea.

Possono essere classificati anche come attivi o passivi: i primi richiedono una fonte energetica per funzionare gli altri no. Inoltre vi sono sensori in commercio destinati a un grande pubblico attraverso dispositivi indossabili e altri destinati a un vero utilizzo in ambienti medici, perché molto più affidabili.
Di seguito un elenco dei sensori non invasivi progettati per l'effettivo utilizzo in ambito ospedaliero e il monitoraggio medico :

- Sensore di temperatura: la temperatura corporea dipende molto dalla parte del corpo in cui avviene la misurazione. In certe situazioni mediche è molto importante misurare la temperatura corporea, perché un certo numero di malattie sono accompagnate da cambiamenti caratteristici della temperatura corporea. In più, al decorso di alcune malattie, si può tenere monitorato il paziente misurandone la temperatura corporea e constatare l'effettiva efficacia del trattamento. I sensori di temperatura sono sensori passivi e non invasivi che vanno applicati in apposite aree del corpo caratterizzati da una parte metallica dalla quale, una volta posizionata sulla pelle del paziente, avviene il campionamento dei dati termici.
- Sensore EMG: l'EMG o elettromiogramma è utilizzato per la diagnosi e l'identificazione di malattie neuromuscolari, per la chinesiologia e per la ricerca di disturbi del controllo motorio. L'elettromiografia è una tecnica utilizzata per la misurazione dell'attività elettrica prodotta dai muscoli a riposo e durante una contrazione. Il sensore EMG utilizza l'elettromiografia per misurare l'attività elettrica filtrata e rettificata del

muscolo su cui `è posto e l'impiego di più sensori possono tener monitorata la condizione neuromuscolare del paziente.

- Sensore ECG: sensore ECG o sensore per l'elettrocardiogramma è molto utilizzato per la diagnosi di molte patologie cardiache, misura l'orientamento del cuore nella cavità toracica ed è utilizzato per la ricerca di evidenze di ipertrofia o danni alle varie parti del muscolo cardiaco. Molte patologie richiedono un continuo monitoraggio del battito cardiaco anche fino a ventiquattro ore e per questo viene applicato il sensore al paziente per ottenere una registrazione continuata della condizione del proprio cuore senza dover restare in ospedale attaccato a una macchina. Il sensore presenta degli elettrodi che vengono posizionati sul petto del paziente per rilevare la frequenza cardiaca. La precisione dell'ECG dipende dalla condizione sottoposta al test: alcune condizioni cardiache non producono modifiche nell'ECG quindi il problema potrebbe non essere sempre visualizzato.
- Sensore del flusso d'aria: è un dispositivo utilizzato per la misurazione della frequenza respiratoria del paziente. Le variazioni anormali di questa frequenza sono indicatrici di grave instabilità fisiologica e in molti casi il tasso di respiratorio `e uno dei primi indicatori di questa problematica. Il sensore `e composto da una serie di poli che vanno posti nelle narici del paziente e da questi poli viene misurata la respirazione.
- ABPM (monitoraggio ambulatoriale della pressione sanguigna): la pressione sanguigna `e la pressione del sangue nelle arterie e viene registrata tramite due valori: pressione sistolica, ossia come batte il cuore, e pressione diastolica, ossia il rilassamento del cuore tra i vari battiti. Tenere monitorata la propria pressione anche a casa è molto importante per molte persone soprattutto quelle che soffrono di ipertensione. L'ipertensione, o pressione alta, può portare problemi come infarto, ictus o malattie renali. Tenendo monitorato un paziente a intervalli regolari per un periodo di ventiquattro o quarantotto ore tramite un specifico dispositivo indossabile si può raccogliere un campione significativo di dati relativo alla pressione sanguigna del paziente durante una sua tipica giornata. Il dispositivo ABPM presenta un bracciale per

la rilevazione della pressione sanguigna e va indossato attorno al braccio e fissato con il velcro.

- Pulsiossimetro SpO2: il pulsiossimetro è un dispositivo che permette di misurare in maniera non invasiva la saturazione arteriosa di ossigeno dell'emoglobina. Il sensore pulsiossimetro è utile per valutare l'ossigenazione del sangue del soggetto e determinare l'efficacia o la necessità di ossigeno supplementare in ambienti e situazioni che ne potrebbero portare a uno stato instabile come: situazioni di terapia intensiva, operazioni o anche piloti in aerei non pressurizzati.
- Glucometro: il glucometro è un dispositivo per determinate la concentrazione di glucosio nel sangue e tenere monitorato questo parametro è molto importante per pazienti che soffrono di diabete.

Questi sensori saranno collegati a uno o più hub che fungono da nodo intermedio per la raccolta dei dati. Questo hub in ambito medico è rappresentato da un monitor che è un'apparecchiatura medica utilizzata per visualizzare i parametri vitali prelevati dai diversi sensori applicati sul paziente. Oggigiorno gli ospedali che utilizzano già questi dispositivi per il monitoraggio del paziente scaricano i dati in loco, ad esempio nell'ambulatorio del medico. La visione 4.0 prevede che i dati raccolti possano essere inviati a un sistema di salvataggio cloud comodamente da casa del paziente durante il periodo di monitoraggio. Questo richiede una comunicazione wireless tra il monitor e il punto di accesso alla rete Internet casalingo. Successivamente queste informazioni verranno analizzati da sistemi di analisi dati e poi dal personale medico per diversi scopi come trarne diagnosi mediche.

11.3. Robotica

L'utilizzo di robot in medicina non risale a molto, però negli ultimi anni vi è stato uno sviluppo tale che oggi è possibile controllare bracci robotici e altre funzionalità da remoto tramite un pannello di controllo e impiegarli per operazioni di chirurgia di precisione. Questi robot non sono ancora completamente automatizzati e sono progettati per offrire un supporto all'attività chirurgica e migliorare le abilità del chirurgo portando in sala operatoria, ad esempio, un braccio meccanico completamente privo di tremolii involontari, dei quali una mano è affetta. I

robot chirurgici non andranno a sostituire la figura del chirurgo, ma ne miglioreranno le capacità dando alla figura medica destrezza, visione e guida di navigazione che vanno al di là di ciò che l'essere umano è capace di fare da solo. Ciò consentirà a sempre più pazienti di accedere a interventi chirurgici minimamente invasivi anche grazie alla realizzazione di dispositivi di diametro inferiore al millimetro con robuste parti mobili, che permettono manipolazioni su microscala e abbastanza forti da interagire con i tessuti . Inoltre, migliorando le capacità del chirurgo si riduce il tempo di ricovero dei pazienti abbattendo di conseguenza la necessità di ricorrere a trasfusioni e diminuendo l'incidenza di complicazioni .

11.4. Realtà Aumentata e Realtà Virtuale

In questa sezione verranno presentati gli usi della realtà aumentata e della realtà virtuale in ambito chirurgico e didattico.

Chirurgia

Uno dei grossi problemi in ambito chirurgico è legato al limitato campo visivo e alla scarsa percezione della profondità che le strumentazioni odierne in possesso agli ospedali offrono al chirurgo. La realtà aumentata può venire in aiuto con una visione in tempo reale della scena operatoria reale migliorata da suoni, video, grafici e altri dati di diverso genere. Più nello specifico il suo potenziale può essere espresso nella chirurgia mininvasiva (MIS), come la laparoscopia, la torascopia e l'endoscopia, grazie alle sue prestazioni computazionali e alla precisione nell'affrontare scene di MIS impegnative. Mentre questa offre notevoli vantaggi rispetto alla chirurgia invasiva, impone anche grandi sfide sulle prestazioni dei chirurghi a causa dei problemi legati al campo visivo, al disallineamento mano-occhi e al disorientamento. Passando cos`ı dal tradizionale metodo di visualizzazione, dove il chirurgo guarda ciò che sta facendo su uno schermo, avendo di conseguenza un disallineamento mano-occhi, a un nuovo metodo, dove le nuove tecnologie AR permettono al professionista di guardare "attraverso" lo schermo. In un prossimo futuro i supporti per l'AR possono essere impiegati anche in altri ambiti medici. Un algoritmo sviluppato dal MIT ha dimostrato come una normale fotocamera per cellulari può rilevare con precisione l'impulso vitale di una persona . L'applicazione di una versione migliorata di questo algoritmo su un dispositivo AR potrebbe essere in grado di

stabilire se un individuo che è collassato ha recuperato un impulso vitale o meno. I rapporti medico-paziente possono essere facilitati e migliorati con, ad esempio, l'utilizzo di codici QR nelle varie postazioni dei pazienti in modo tale che il medico riceva le informazioni rilevanti guardando semplicemente il codice attraverso il dispositivo AR .

Formazione

La nuova modalità di visione della realtà aumentata permette agli studenti di chirurgia, soliti a imparare osservando da oltre le spalle del chirurgo, di vedere direttamente ciò che sta guardando il chirurgo che indossa il supporto per la realtà aumentata dato che il suo punto di vista può essere riprodotto o proiettato contemporaneamente su altre piattaforme o dispositivi. Per quanto riguarda la realtà virtuale (VR) è stata utilizzata per decenni per la formazione e l'allenamento endoscopico dei nuovi chirurghi data la sua capacità di generare un'immagine immersiva e completamente artificiale conla possibilità di interazione in tempo reale con un ambiente virtuale.

11.5. Gestione ed elaborazione dati

Un intero sistema basato sul'IoT come l'Ospedale 4.0 presenta un enorme quantitativo di dispositivi collegati in rete che producono un'altrettanta mole di dati che devono essere memorizzati, gestiti e analizzati. I servizi di cloud computing offrono un'ampia interoperabilità e integrazione con il mondo IoT, permettendo il salvataggio e la gestione dei dati provenienti dai vari dispositivi. Inoltre questi servizi possono consentire l'accesso remoto alle applicazioni e ai dati via Internet utilizzando sistemi cablati e non, in qualsiasi momento e da qualsiasi luogo in cui ci sia la possibilità di avere accesso a Internet. Il vantaggio funzionale più grande che i vari servizi di cloud computing possono offrire è l'assistenza sanitaria, dato che offrono l'opportunità di estendere le capacità disponibili al personale dell'organizzazione sanitaria, al fine di implementare modi migliori di lavorare e offrire nuovi servizi ai pazienti .

Un sistema che si basa sullo scambio e trasmissione dei dati come questo ha bisogno di un'unità di elaborazione locale per il filtraggio dei dati, la compressione dei dati, la fusione dei dati e l'analisi dei dati . Nella fase di filtraggio avviene una pre-elaborazione dei dati

provenienti dai vari sensori andando a rimuovere alcuni rumori accumulati nei biosegnali come: oscillazioni di corrente alternata nella rete elettrica, interferenze elettroma-gnetiche da altri dispositivi elettrici e collegamento improprio dei sensori al corpo dei pazienti. Nonostante ci sia già un filtraggio leggero durante la fase di raccolta dei dati, è necessario un secondo filtraggio più robusto lato cloud. La seconda fase, quella di compressione, comporta la riduzione delle dimensioni dei dati e può essere senza perdita (lossless) o con perdita (lossy) dove quest'ultima è più adatta per quei sensori con risorse limitate quali durata batteria e capacità di elaborazione. Per tutti i sensori che monitorano parametri vitali i quali dati devono avere tutte le caratteristiche dei segnali osservabili con una precisione elevata, come l'ECG, `e consigliato un approccio senza perdita . La compressione comporta meno latenza delle comunicazioni, transazioni meno energivore e meno tempo per l'elaborazione dei dati. La fase di fusione consente la riduzione del volume dei dati integrando i dati di più sensori per produrre informazioni più coerenti, accurate e utili rispetto a quelle fornite da ogni singolo sensore. Infine chiude il ciclo della gestione dei dati con la fase di analisi. Analisi che in un'ottica 4.0 deve essere automatizzata con tecniche di apprendimento e big data e affiancata al personale sanitario per accompagnare il medico nel supporto decisionale . Negli ultimi anni si sono fatti grandi passi nell'intelligenza artificiale applicata all'ambito sanitario. Ogni giorno i pazienti soffrono di condizioni mediche che possono degenerare fino alla morte, perché non ricevono i trattamenti giusti in maniera tempestiva. Oggi il personale medico non dispone di strumenti che possano velocizzare in mondo significativo il processo decisionale. L'applicazione di queste tecniche di intelligenza artificiale sembrano essere ciò che la medicina cerca permettendo l'analisi di ogni risultato dei test e la determinazione del trattamento più giusto in tempi molto brevi, consentendo a un paziente che ha bisogno di cure mediche complesse o urgenti di entrare in contatto con lo specialista giusto immediatamente.

11.6. Sicurezza e Privacy

Come già visto nelle sezioni precedenti il modello ospedaliero 4.0 prevede l'adozione dell'IoT che pervaderà l'intero ambiente tramite dispositivi integrati ai vari processi. Questi dispositivi e le varie applicazioni sanitarie si occuperanno di informazioni estremamente private come i dati sanitari dei pazienti. Inoltre, tali dispositivi saranno collegati alla rete interna dell'ospedale

e alcuni di essi saranno pure interfacciati alla rete Internet per poter dare accesso alle informazioni in qualunque momento e in qualunque luogo alle persone autorizzate . Pertanto l'interno dominio sanitario IoT per le informazioni che contiene sarà un bersaglio appetibile da malintenzionati e potrà essere soggetto a molteplici attacchi informatici. E` fondamentale quindi capire quali sono i requisiti di una rete IoT che deve avere in termini di sicurezza e quali sfide porta il loro utilizzo nella sicurezza. I requisiti di sicurezza di un sistema sanitario basato sugli IoT sono molto simili agli scenari standard di comunicazione. Si possono pertanto suddividere nelle seguenti categorie.

- Riservatezza: garantisce l'inaccessibilità delle informazioni mediche dei pazienti agli utenti non autorizzati.
- Integrità: garantisce l'inalterabilità a dei dati sanitari dei pazienti.
- Autenticazione: consente a un dispositivo IoT di stabilire l'identità del nodo con cui sta comunicando.
- Disponibilità : garantisce la normale fruizione dei servizi sanitari che la rete IoT offre agli autorizzati anche sotto attacco.
- Non ripudio: garantisce che un nodo non può ripudiare la paternità di un messaggio già inviato.
- Autorizzazione: garantisce che solo i nodi autorizzati siano accessibili per servizi o risorse di rete.
- Capacità di recupero: come si può intuire si tratta della capacità di ritornare allo stato di normale attività seguito di un'interruzione causata da un attacco o altri fattori. Non solo: garantisce anche, a seguito della compromissione di una parte della rete, la protezione dei dati, dei dispositivi e della restante rete non compromessa.
- Tolleranza degli errori: prevede che il sistema continui a fornire i servizi di sicurezza anche in presenza di guasti.
- Auto ripresa: quando un dispositivo all'interno della rete smette di funzionare gli altri dispositivi rimanenti devono rendere possibile un livello minimo di sicurezza.

12. Acronimi

6Lo IPv6 over Networks of Resource Constrained Nodes

6LoWPAN IPv6 over Low Power Wireless Personal Area Networks

6TiSCH IPv6 over Time Slotted Channel Hopping Mode of IEEE 802.15.4e

AMQP The Advanced Message Queuing Protocol

CoAP Constrained Application Protocol

CoRE Constrained RESTful Environment

DASH7 Named after last two characters in ISO 18000-7

FDMA Frequency division multiple access

GHz Giga Hertz

HART Highway Addressable Remote Transducer Protocol

IEEE Institution of Electrical and Electronic Engineers

IETF Internet Engineering Task Force

IoT Internet of Things

IP Internet Protocol

IPv6 Internet Protocol version 6

ISM Industrial, Scientific and Medical frequency band

ITU-T International Telecommunications Union - Telecommunications

ITU International Telecommunications Union

L2CAP Logical Link Control and Adaptation Protocol

LoRaWAN Long Range Wide Area Network

LTE-A Long-Term Evolution Advanced

LTE Long-Term Evolution

M2M Machine to Machine

MAC Media Access Control

MQTT Message Queue Telemetry Transport

OASIS Advancing Open Standards in the Information Society

OFDM Orthogonal Frequency Division Multiplexing

OMG Object Management Group

PHY Physical Layer

QoS Quality of Service

RAN Radio Access Network

Networking Protocols and Standards for Internet of Things

REST Representational State Transfer

RESTful Representational State Transfer based

RFC Request for Comments

RFID Radio-frequency identification

RPL Routing Protocol for Low-Power and Lossy Networks

SIG Special Interest Group

SMQTT Secure MQTT

SOA Services Oriented Architecture

SSL Secure Socket Layer

TCP Transmission Control Protocol

TDMA Time Division Multiple Access

TLS Transport Level Security

TSCH Time-Slotted Channel Hopping

UDP User Datagram Protocol

WiFi Wireless Fidelity

WirelessHART Wireless Highway Addressable Remote Transducer Protocol

WPAN Wireless Personal Area Network

XML Extensible Markup Language

XMPP Extensible Messaging and Presence Protocol

13. Riferimenti

Sono di seguito indicati alcuni dei documenti consultati sul tema IoT. L'elenco non esaurisce i temi, permette tuttavia di accedere all'enorme patrimonio informativo e formativo disponibile sul World Wide Web.

1. Alliance for Internet of Things Innovation – AIOTI (2015) High Level Architecture
2. ETSI (2014) OneM2M Architecture Analysis
3. ETSI (2013) M2M Communication M2M Service Requirement
4. GSMA (2015) GSMA IoT Security Guidelines
5. IEEE (2016) IEEE IoT Standard Development
6. IEEE-SA (2015) Internet of Things Ecosystem Study
7. IERC (2015) Internet of Things beyond the Hype
8. IETF (2013) 6LoWPAN book
9. ISO –IEC (2016) IoT WG10 Reference Architecture - draft
10. ISO –IEC (2014) Study Report on IoT Reference Architecture / Framework
11. ITU-T (2012) Overview of Internet of Things Y 2060
12. ITU-T (2013) Framework of Web of Things Y 2063N
13. NIST (2015) Framework of Cyber Physical System Rel. 0.7
14. Alleseen Alliance (2014) Introduction to AllJoyn Framework
15. Bluetooth (2016) Bluetooth Core Specification v.5
16. CSCC (2016) Cloud Customer Architecture for IoT
17. Continua Alliance (2015) Interoperability Design Guidelines for Personal Health System
18. Ericsson (2016) White Paper 5G Radio Access
19. Ericsson (2016) White Paper Cellular Networks for Massive IoT
20. Huawei (2013) 5G A Technology Vision
21. Industrial Internet Consortium – IIC (2015) Industrial Internet Vocabolary
22. IoT World Forum (2014) Building the Internet of Things
23. IPSO Alliance (2011) 6 LoWPAN RPL Protocol
24. Machina Research – Lora Alliance (2014) LPWA Technologies
25. NGMN (2015) NGMN 5G White Paper
26. Online Trust Alliance (2016) OTA- IoT Trust Framework
27. Siemens (2012) Industrial Wireless Communication
28. SigFox (2014) M2M and IoT redefined through cost effective and energy optimized connectivity
29. Thread Group (2015) Thread Stack Framework
30. World Economic Forum (2015) Industrial Internet of Things
31. Zigbee (2011) Zigbee Smart Energy 2.0