ALMA MATER STUDIORUM - UNIVERSITÀ DI BOLOGNA

SCUOLA DI INGEGNERIA E ARCHITETTURA

CORSO DI LAUREA IN INGEGNERIA INFORMATICA T

TESI DI LAUREA

in

Laboratorio Di Amministrazione Di Sistemi T

La sicurezza nell'Internet of Things

CANDIDATO
Mauro Cherchi

RELATORE:
Prof. Marco Prandini

Anno Accademico 2014/15

Sessione III

La sicurezza nell'Internet of Things

Mauro Cherchi

7 marzo 2016

Indice

Capitolo 1

Breve introduzione all'IoT

L'internet delle cose è la più grande rivoluzione introdotta dalla rete globale negli ultimi tempi, si propone di fondere il mondo reale con quello virtuale creando un ambiente più intelligente. Un ambiente in grado di sentire, analizzare e adattarsi per rendere le nostre vite più semplici, sicure ed efficienti.[1]

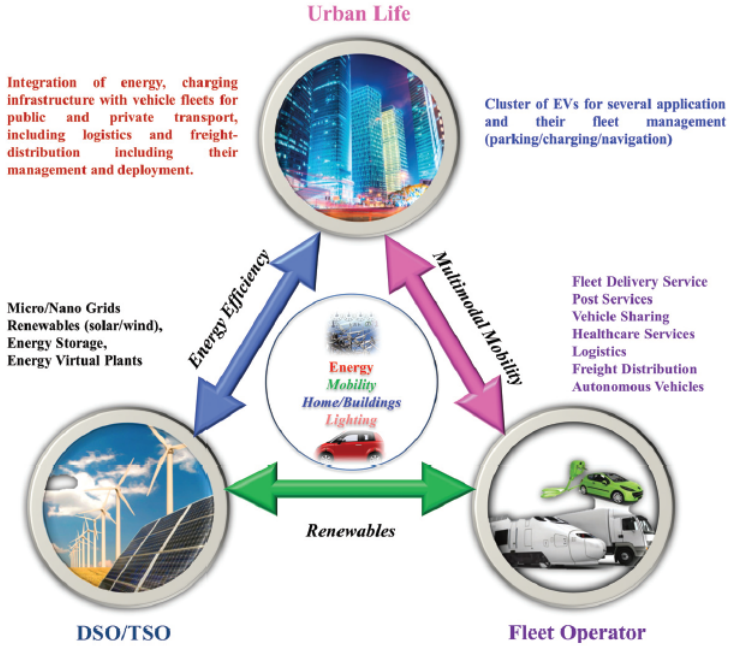


Figura 1.1: IoT Application Sectors [1]

Non si tratta di una nuova campagna pubblicitaria sulla tecnologia ma di una realtà composta da un infinità di piccole e grandi iniziative che sfruttando le nuove tecnologie sono in grado di cambiare totalmente tutti gli aspetti

della nostra vita. Esistono tantissimi casi d'uso, dalle case intelligenti alla gestione di impianti di produzione industriale, dal monitoraggio e miglioramento di coltivazioni e allevamenti all'utilizzo in campo militare, da sistemi di scala globale a piccoli ambienti. Le grandi case, leader nel settore informatico, stanno sviluppando framework e soluzioni per l'implementazione e la messa in opera delle nuove possibilità offerte da questo nuovo mercato, investendo ingenti somme per non farsi sfuggire questa opportunità in piena fase di definizione e sviluppo.

1.1 Storia ed espansione

Nei primi anni 2000 nei laboratori "AutoID" del MIT venivano poste le basi per il concetto che sarebbe diventato la visione dell'internet delle cose, Kevin Ashton[2] in un articolo del RFID Journal scrisse: "*If we had computers that knew everything there was to know about things-using data they gathered without any help from us – we would be able to track and count everything, and greatly reduce waste, loss and cost. We would know when things needed replacing, repairing or recalling, and whether they were fresh or past their best. We need to empower computers with their own means of gathering information, so they can see, hear and smell the world for themselves, in all its random glory. RFID and sensor technology enable computers to observe, identify and understand the world-without the limitations of human-entered data.*" [3][4]

Il concetto era semplice e potente, se tutti gli oggetti della vita di ogni giorno fossero stati equipaggiati con identificatori e connettività wireless, questi oggetti avrebbero potuto comunicare tra di loro ed essere gestiti dai computer. A quel tempo non erano disponibili le tecnologie necessarie per realizzare questa visione e l'idea, per quanto allettante, rimase una visione futuristica. Successivamente vi fù un periodo di calma dove gli interessati all'argomento rimasero "in pochi" più che altro come forma di ricerca.[5]

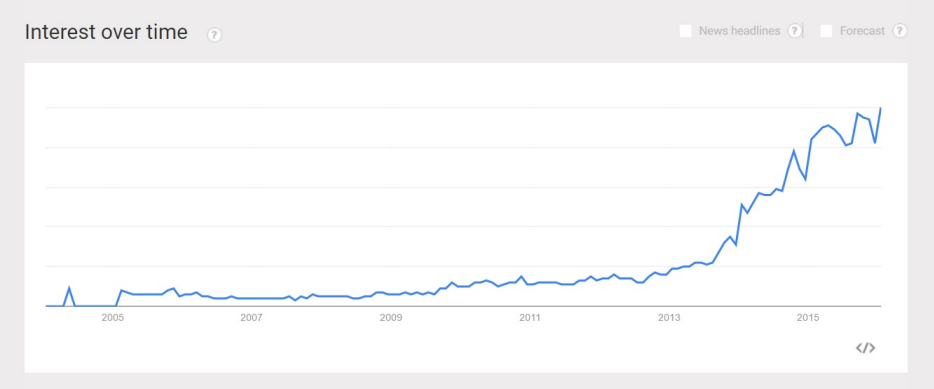


Figura 1.2: Interest over tyme [6]

Negli ultimi anni successivamente allo sviluppo di nuove tecnologie (vedi Sez. 1.3.3) questa visione è diventata realizzabile con costi sostenibili/ragionevoli. Sono infatti nate diverse organizzazioni (AIOTI, IERC, IOT-WF ...) che assieme alle vecchie (IEEE, ISO, ITU ...) si propongono di promuovere, facilitare, guidare lo sviluppo di questo concetto garantendone tra le altre cose la sicurezza. Proprio questo argomento è stato uno degli ultimi ad essere affrontato, forse perché va in conflitto con gli attori di mercato che puntano a raccogliere più dati possibile e nel modo più mirato possibile sui consumatori.[7] Tuttavia sono stati messi in cantiere diversi progetti pilota, alcuni dei quali particolarmente mirati a studiare proprio le problematiche sulla sicurezza (verranno trattati nella sezione 2.3).

1.2 Trend di Mercato

Da recenti previsioni fatte dall'"International Data Corporation" (IDC) il valore di mercato dell'IoT, nella sola Unione Europea dovrebbe superare i mille miliardi (10^{12}) di euro entro il 2020.[8]

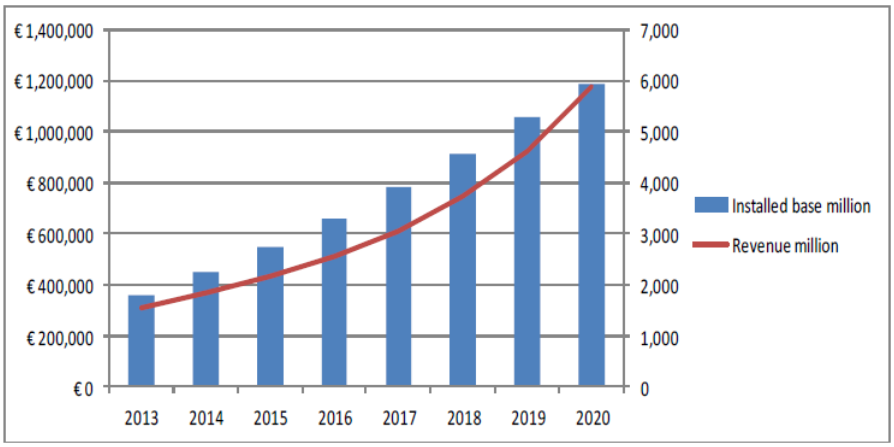


Figura 1.3: IoT Installed Base and Revenues in EU [8]

Tutti trend tecnologici per il 2016 individuati nel Gartner Symposium/ITxpo tenutosi ad Orlando il 6 Ottobre 2015 hanno a che vedere direttamente o indirettamente con l'IoT. Si parla di una crescita di endpoint da utilizzare per interagire con persone cose ed enti utilizzando la rete, realtà aumentata, sistemi per la gestione delle informazioni in grado di far fronte alla sempre maggiore quantità di informazioni prodotta dai dispositivi, "Machine Learning" e macchine autonome (concrete come robot o virtuali come Google now e Siri). Ancora, sistemi di sicurezza adattivi e nuove architetture per tutelare le nuove tecnologie come appunto l'IoT.[9]

IoT avrà un impatto su tutti i settori produttivi ma alcuni di questi faranno investimenti decisamente maggiori rispetto ad altri, ci si aspetta che quelli che approfitteranno prima e investendo di più, saranno quelli che hanno fatto lo stesso con le "vecchie" tecnologie informatiche. In figura 1.4 e 1.5 due schemi con gli investimenti previsti nei prossimi anni divisi per settore produttivo.

Country	2014	2020
Agriculture, construction, and mining	€ 7 311	€ 23 193
Business services	€ 28 334	€ 90 218
Communications	€ 37 388	€ 119 975
Education & Health	€ 22 060	€ 66 925
Finance	€ 73 709	€ 242 222
Local & Central Government	€ 49 742	€ 153 707
Manufacturing	€ 87 805	€ 286 539
Retail & Wholesale	€ 38 024	€ 124 412
Transport	€ 8 659	€ 27 728
Utilities	€ 10 630	€ 39 668
Others	€ 2 330	€ 7 017
Total	**€ 365 992**	**€ 1 181 603**

Figura 1.4: IoT Market Size and Forecast: Baseline Scenario by Vertical Market (€Million) [8]

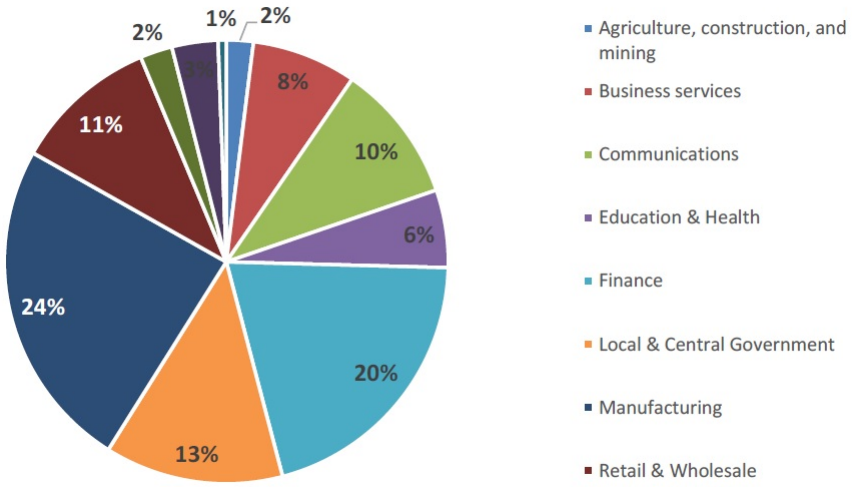


Figura 1.5: IoT Market Size and Forecast: Baseline Scenario by Vertical Market (2020; %) [8]

Le maggiori attrattive di business si possono raggruppare in 4 macro argomenti: "Smart Manufacturing", "Smart Homes", "Smart Health" e "Smart Customer Experience". Questi dati sono stati ottenuti tenendo in considerazione la crescita stimata del settore e la spesa stimata per l'IoT in quel settore.

Il settore "Smart Manufacturing" è in testa rappresentando l'opportunità migliore in termini di spesa nell'IoT, seguito da vicino da "Smart Homes"

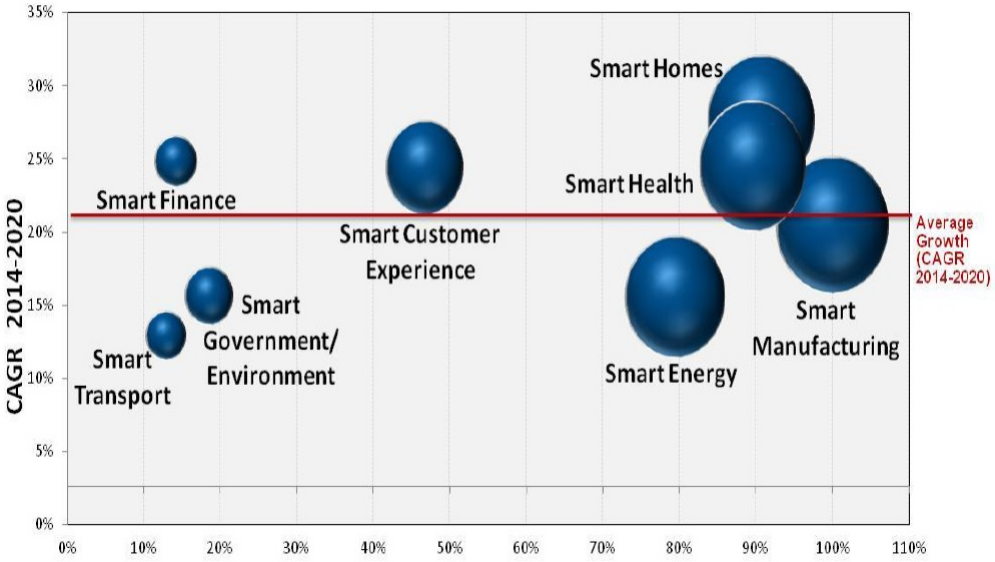


Figura 1.6: Smart Environments by IoT Spending Size and Growth [8]

e "Smart Health" che rappresentano anch'essi un ottimo mercato de tenere in grande considerazione durante lo studio/sviluppo di tutte le tecnologie che andranno a formare l'IoT.[8] Parlando di "case intelligenti" e "salute intelligente" si nota subito quanto possa essere importante studiare ed approfondire le tematiche di messa in sicurezza delle tecnologie che andranno ad incidere su ambiti così importanti della nostra vita.

1.3 Definizione

ITU-T: "*A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies.*
NOTE 1 - Through the exploitation of identification, data capture, processing and communication capabilities, the IoT makes full use of things to offer services to all kinds of applications, while ensuring that security and privacy requirements are fulfilled.
NOTE 2 - From a broader perspective, the IoT can be perceived as a vision with technological and societal implications."[10]

IERC: "*A dynamic global network infrasturcture with self-configuring capabilities based on standard and iteroperable communication protocols where physical an virtual "things" have identities, physical attributes, and virtual personalities and use intelligent interfaces, and are seamlessly integrated into the information network.*"[11]
Un infrastruttura globale che permetta a servizi avanzati di connettere cose (fisiche e virtuali), basata sulle tecnologie di comunicazione esistenti e in evoluzione.

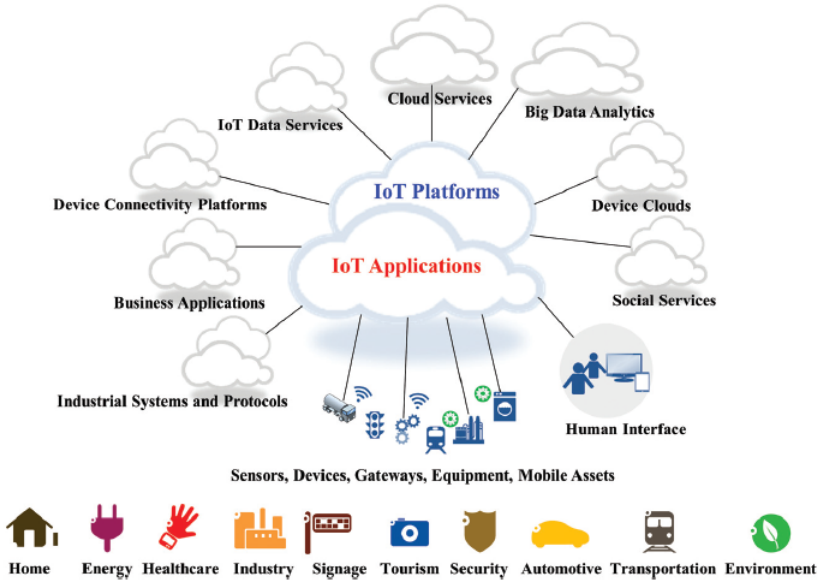


Figura 1.7: IoT Integration [1]

1.3.1 Architettura

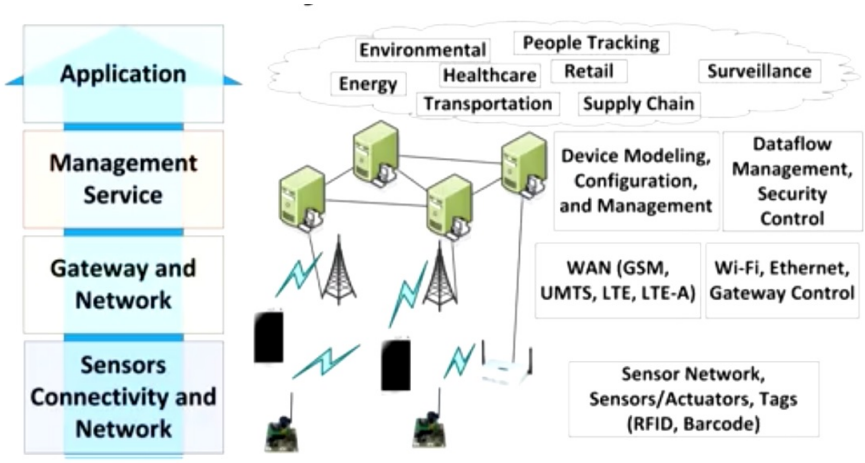


Figura 1.8: IoT Architecture [12]

L'architettura può essere suddivisa in 4 livelli concettuali, dal più vicino fisicamente all'utente, al contesto, "alle things", a quello più lontano, distribuito "astratto". Alcuni di questi layer logici possono essere tuttavia implementati contemporaneamente su diversi layer fisici (es: un RFID sicuramente implementa soltanto il primo livello, mentre uno smartphone può implementarli tutti) [Fig. 1.8]

Partendo dal basso, dal layer "Sensors Connectivity and Network", si trovano gli oggetti che raccolgono dati o che "attuano" dei comportamenti nel contesto reale (Smart Home, Smart Company ...). Ne fanno quindi parte tecnologie come RFID, Barcode, NFC, smartphone e qualsiasi dispositivo in grado di raccogliere informazioni sull'ambiente circostante o di attuarvi dei comportamenti. Alcuni di questi dispositivi (per esempio quelli che usano tecnologia NFC) si devono appoggiare a dispositivi "più potenti" (Gateway) per trasmettere/ricevere dati dal network/internetwork, altri invece sono in grado di connettersi direttamente sia alle LAN che alle WAN (per esempio gli smartphone). A questo livello le tecnologie utilizzate per stabilire connessioni e comunicare sono principalmente UWB, ZigBee, Bluetooth, 6LowPan o semplicemente connessioni wired. [Fig. 1.9]

Il livello immediatamente sopra, "Gateway-Network" è quello che permette ai dispositivi meno potenti di collegarsi alla rete locale e a quelli più potenti (trai quali anche i dispositivi di gateway) di collegarsi all'internetwork. I protocolli di comunicazione più utilizzati sono: Wi-Fi ed Ethernet per le LAN (Network) e 3G, LTE ed LTE-A per le WAN (Internetwork). Questo layer permette di collegare assieme tutte le things e quindi raccogliere i dati

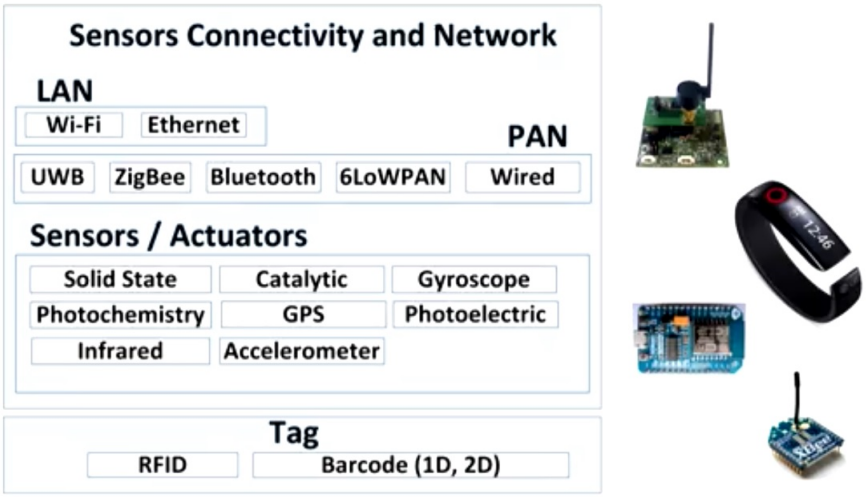


Figura 1.9: IoT Architecture - Sensor layer [12]

per fornirli ai livelli superiori dove vengono utilizzati per offrire servizi complessi, oppure in direzione opposta, permettono alle things di ottenere dati dai servizi per agire di conseguenza nel contesto nel quale operano. [Fig. 1.10]

Figura 1.10: IoT Architecture -Network layer [12]

Tra il livello di gateway/network sottostante e quello dei servizi/cloud sovrastante, vi è un livello logico intermedio. Su questo livello, quello di gestione servizi, si posizionano tutte quelle tecnologie/tecniche che permettono la gestione del network e dei dati stessi che vi circolano. Questo livello può essere stratificato su diversi network e parte di questo livello può far parte anche dei dispositivi più potenti del livello inferiore, quelli con capacità computazionali sufficienti.[Fig. 1.11]

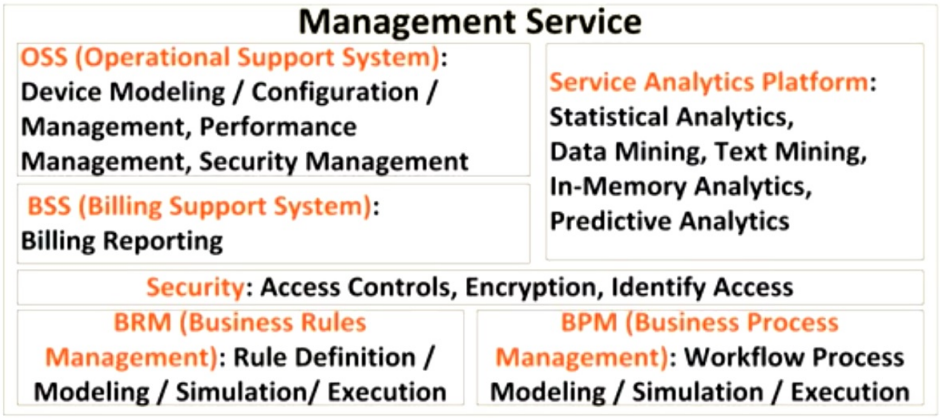


Figura 1.11: IoT Architecture - Management services layer [12]

Il livello più alto, anche questo potenzialmente stratificato su più layer o distribuito in più punti dello stesso, è quello che analizzando ed elaborando i dati forniti dalle things fornisce servizi che verranno utilizzati dalle stesse o da altre applicazioni. A questo livello appartengono le funzionalità di Fog-computing e Cloud-computing.[Fig. 1.12]

Figura 1.12: IoT Architecture - Applications layer [12]

1.3.2 Network

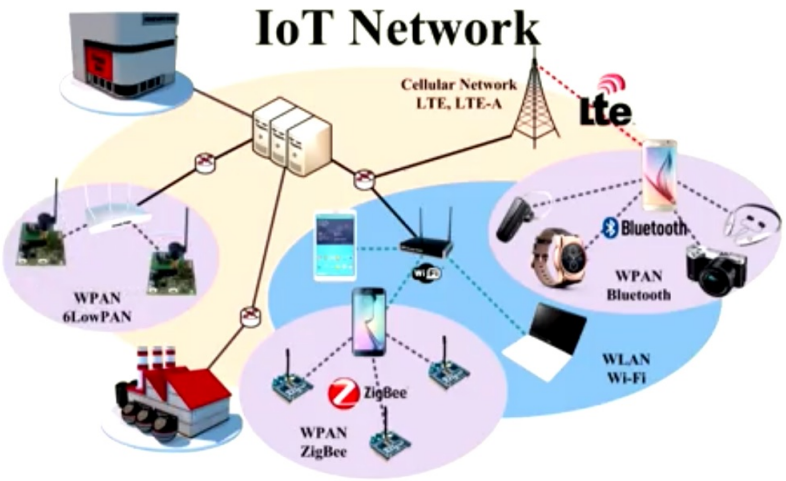


Figura 1.13: IoT Network [13]

La struttura dei network che verranno formati può essere suddivisa in tre macro categorie a seconda della loro estensione geografica: PAN, LAN e WAN. [Fig. 1.13]

PAN Personal Area Network: si prevede che in a questo livello le principali tecnologie utilizzate faranno parte delle WPAN (Wireless Personal Area Network). Sfruttando gli smartphone come gateway, le things vi si connetteranno utilizzando protocolli tra i quali:

- **RFID** Piccoli tag che attraverso i campi magnetici possono essere riconosciuti da appositi lettori. Possono essere energeticamente passivi (alimentati dal campo del lettore) o contenere piccole batterie e comunicare piccole informazioni a centinaia di metri dai lettori.[14]
- **NFC** Protocollo di comunicazione che permette ai dispositivi dotati di questa tecnologia di connettersi tra di loro ad una distanza di circa 10 cm. ad una velocità dai 106 ai 424 kbit/s.[15]
- **ZigBee** Insieme di protocolli di comunicazione di livello network conformi allo standard IEEE 802.15.4 (opera su layer sottostanti conformi allo stesso standard) sviluppati per soddisfare requisiti di basso consumo energetico e prezzo. Se tra di loro non vi sono ostacoli, i dispositivi sono in grado di comunicare ad una distanza massima di 100 metri ad una velocità massima di 250 kbit/s.[16]

- **6LowPAN** Acronimo di "IPv6 over Low power Wireless Personal Area Networks".[17] È uno standard sviluppato dal IERC con l'obiettivo di permettere anche ai dispositivi a basso consumo energetico di utilizzare lo standard IPv6 specificato nel RFC 2460 e successive integrazioni.[18]
- **Bluetooth**

LAN Local Area Network: anche in questo caso la tendenza è verso tecnologie wireless, qundi principalmente standard Wi-Fi IEEE 802.11 oppure Ethernet IEEE 802.3.

WAN A questo livello l'unico cambiamento degno di nota sembra essere il notevole incremento del traffico sulle reti utilizzate dai dispositivi mobili quali: **GSM**[19], **UMTS**[20], **LTE**[21], **LTE-A**[22]. Si inizia a parlare anche di reti 5G per le quali ancora non sono stati definiti standard.[1]

Communication Technologies

	NFC	RFID	Blue-tooth®	Blue-tooth® LE	ANT	Proprietery (Sub-GHz & 2.4 GHz)	Wi-Fi®	ZigBee®	Z-wave	KNX	Wireless HART	6LoWPAN	WiMAX	2.5–3.5 G
Network	PAN	PAN	PAN	PAN	PAN	LAN	LAN	LAN	LAN	LAN	LAN	LAN	MAN	WAN
Topology	P2P	P2P	Star	Star	P2P, Star, Tree Mesh	Star, Mesh	Star	Mesh, Star, Tree	Mesh	Mesh, Star, Tree	Mesh, Star	Mesh, Star	Mesh	Mesh
Power	Very Low	Very Low	Low	Very Low	Very Low	Very Low to Low	Low-High	Very Low	Very Low	Very Low	Very Low	Very Low	High	High
Speed	400 Kbs	400 Kbs	700 kbs	1 Mbs	1 Mbs	250 kbs	11-100 Mbs	250 kbs	40 Kbs	1.2 Kbps	250 kbs	250 Kbs	11-100 Mbs	1.8-7.2 Mbs
Range	<10 cm	<3 m	<30 m	5-10 m	1-30 m	10-70 m	4-20 m	10-300 m	30 m	800 m	200 m	800 m (Sub-GHz)	50 km	Cellular network
Application	Pay, get access, share, initiate service, easy setup	Item tracking	Network for data exchange, headset	Health and fitness	Sports and fitness	Point to point connectivity	Internet, multimedia	Sensor networks, building and industrial automation	Residential lighting and automation	Building automation	Industrial sensing networks	Senor networks, building and industrial automation	Metro area broadband Internet connectivity	Cellular phones and telemetry
Cost Adder	Low	Low	Low	Low	Low	Medium	Medium	Medium	Low	Medium	Medium	Medium	High	High

Figura 1.14: IoT Wireless Communication Tchnologies [23]

I dispositivi che costituiscono PAN e LAN si possono dividere in due macro categorie: **FFD** e **RFD** (IEEE 802.15.4). I dispositivi che fanno parte della categoria "Full Function Devices" sono tutti quelli che hanno piene capacità di ricezione, invio, instradamento (routing) dei dati e possono implementare funzionalità di "Service Management" [Fig. 1.11]. Questi dispositivi possono fare da coordinatori delle PAN. I dispositivi che invece fanno parte della categoria "Reduced Funcion Devices" sono tipicamente i sensori o gli switch che per entrare a far parte dell'internetwork hanno bisogno di comunicare con i dispositivi FFD. I dispositivi RFD invece non possono mai fungere da coordinatori delle reti PAN.[12][Fig. 2.1]

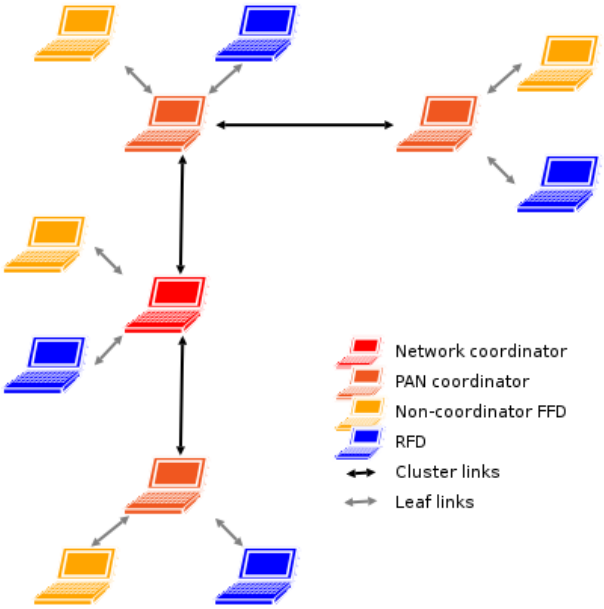


Figura 1.15: IoT Network [24]

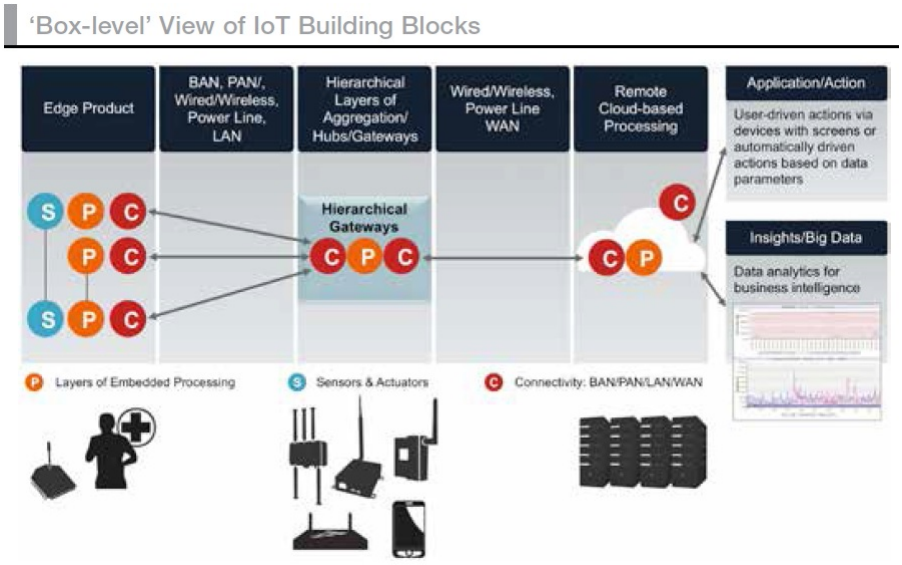


Figura 1.16: IoT Building Blocks [23]

1.3.3 Tecnologie

Perché l'Internet Of Things passi da visione a realtà, oltre alle tecnologie disponibili è necessario che ne vengano sviluppate di nuove.[25][1] Le principali sfide tecnologiche alle quali o si sta già lavorando o si dovrà far fronte nel breve/medio termine sono:

Wireless Sensors Network(s) I dati prodotti dai dispositivi (soprattutto da quelli classificati come RFD) hanno bisogno di essere raccolti, salvati, processati e inviati attraverso sistemi in grado di garantire efficienza, bassi consumi, costi ragionevoli, privacy e sicurezza. Questi dati devono anche essere filtrati per evitare il sovraccarico dei sistemi sovrastanti che potrebbero non supportare la mole di informazioni (dinamica! in quanto non è possibile determinare a priori quanti dispositivi si collegheranno ad un network) oppure perché semplicemente non hanno bisogno di tutte queste informazioni (Edge/Fog computing).

Devices Identification & User Identification Con la crescita spropositata di dispositivi connessi alla rete sono necessari nuovi metodi di identificazione sia dei dispositivi che degli utenti che in quel momento stanno usando i dispositivi. Se per l'identificazione dei dispositivi è stato sviluppato il protocollo IPv6, per l'identificazione degli utenti sono ancora in corso gli studi, c'è chi parla di identificazione basata su parametri biometrici.[26]

Cloud & Edge/Fog computing Il Cloud computing è sicuramente la parte fondamentale dell'IoT, senza la quale la raccolta dei dati sarebbe fine a se stessa, tuttavia per fare in modo che nel cloud arrivino soltanto i dati strettamente necessari all'erogazione dei servizi offerti è necessaria un'operazione di filtro/elaborazione parziale preventiva, nei cosiddetti "Fog" e "Edge", due spazi immaginari che comprendono l'insieme dei dispositivi RFD e FFD dai quali si trova a passare l'informazione prima di raggiungere il Cloud.[Fig. 1.17] Questa elaborazione distribuita serve anche ad alleggerire il carico di lavoro alle macchine che operano nel Cloud, migliorare i tempi di risposta dei servizi e rendere il sistema più elastico/resistente ad eventuali problemi di rete che isolassero le Things dal Cloud. Nella "nebbia" saranno anche implementate funzionalità di controllo degli accessi e "Context awareness".[1]

Federated IoT Data & Large scale services orchestration Per realizzare la visione di grandi sistemi (es. smart city) in grado di raccogliere dati, elaborarli e fornire servizi, c'è bisogno di un coordinamento nello sviluppo/adozione delle nuove tecnologie in modo che queste possano operare ed essere utilizzate in un sistema eterogeneo che sappia astrarre i dati dalle

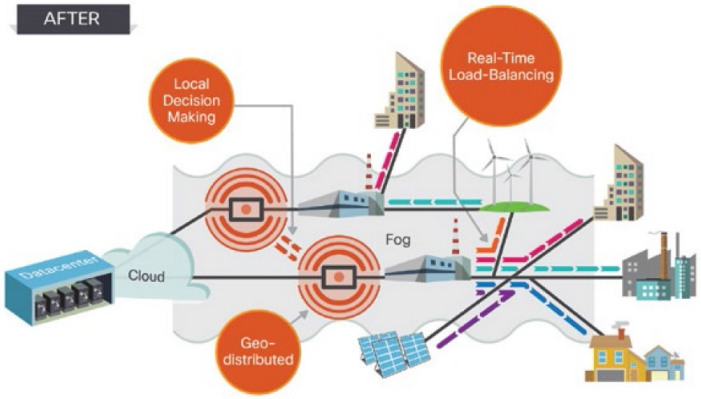


Figura 1.17: Edge & Fog computing [27]

tecnologie dalle quali provengono per poter essere utilizzati uniformemente nella fase di analisi ed elaborazione. È quindi necessario che il middleware IoT fornisca le capacità di auto-configurazione e auto-organizzazione in sistemi/tecnologie diverse offerte da diversi produttori.[1]

IoT Data Analytics Per fare in modo che i dati possano essere analizzati agevolmente è necessario che questi, anche se provenienti da dispositivi eterogenei, abbiano una rappresentazione astratta comune, confrontabile e che la raccolta dei dati avvenga attraverso un middleware dove privacy e sicurezza vengono curati con un cetro livello di garanzia. Una grande spinta si avrà anche sulle tecnologie di Machine Learning e Query Language, oltre allo sviluppo di algoritmi efficienti per l'analisi dei dati raccolti e per l'elaborazione delle informazioni da mandare in risposta ai sistemi.[1]

Interoperability framework I framework dovranno garantire interoperabilità tra i dispositivi, cioé dovranno fornire gli strumetnti necessari affinché i dispositivi possano concordare autonomamente tra di loro quali protocolli, linguaggi e formati usare per trasmettere quali informazioni ed infine come queste debbano essere interpretate.[1]

1.4 Protagonisti in campo

Tra i principali protagonisti in campo come fornitori di dispositivi, servizi e framework di sviluppo si possono elencare:

- **Google** Offre hosting per il deploy di servizi Cloud e BigData Analysis e mette a disposizione servizi "già pronti" come le API di traduzione e geolocalizzazione.[28] Oltre a questo offre strumenti per lo sviluppo tra i quali "Brillo", un sistema operativo basato su Android con installati

servizi mirati all'IoT e un Developer Kit per aggiungervi le funzionalità desiderate.[29] Un altro strumento è Weave, piattaforma che espone API per la gestione della comunicazione device-to-device e device-to-cloud, inoltre questo strumento vanta di essere "Secure by default" attraverso l'utilizzo di controllo accessi e crittografia.[30]

- **Microsoft** L'offerta di Microsoft comprende più che altro soluzioni per il cloud e la gestione dei dispositivi attraverso "Azure IoT Suite".[31]

- **Apple** La casa di Steve Jobs sorprendentemente ha messo a disposizione soltanto HomeKit. Un framework che permette di configurare dispositivi Apple in una smart Home in modo da poterli utilizzare attraverso Siri.[32]

- **Samsung** La direzione, o meglio il settore commerciale al quale punta Samsung, sembra essere quello delle Smart Home. È partita con li lancio di "Smartthings", un'insieme di prodotti per le case intelligenti e ora preannuncia l'arrivo di una famiglia di prodotti appositamente creati per gli sviluppatori, "ARTIK" sul quale creare e sperimentare soluzioni (stile Arduino).[33][34]

- **Cisco** Probabilmente la casa con più soluzioni hardware e software nel portafoglio per la costruzione di sistemi IoT su misura. Fornisce componenti che vanno da piccoli sensori ai server, passando per tutti i dispositivi necessari alla comunicazione ponendo molta attenzione alle questioni di sicurezza.[35]

Capitolo 2

Sicurezza

Tutte le tecnologie viste in precedenza e quelle nuove che verranno sviluppate per far fronte alle sfide poste dall'IoT, dovranno essere messe in sicurezza. Di seguito quindi prima una trattazione generale sul concetto di sicurezza, poi sulle problematiche specifiche del ICT ed infine su quelle introdotte dall'IoT individuate grazie ai progetti pilota.

2.1 Definizione generale

La sicurezza è definita come "Il grado di resistenza a, o protezione da un danno. Si applica a qualsiasi bene, come persone, abitazioni, comunità, cose, nazioni o organizzazioni."[36]

I concetti fondamentali della sicurezza sono:
Minaccia Un intento di azione che se messo in pratica sfruttando una o più vulnerabilità può causare un danno.
Vulnerabilità Una debolezza che può essere utilizzata per mettere in pratica una minaccia.
Exploit Il verificarsi di un rischio attraverso lo sfruttamento di una vulnerabilità.
Rischio La possibilità che si verifichi un evento dannoso.
Contromisura Un metodo per impedire un exploit.
Difesa elastica Pratica del mettere in opera più contromisure su diversi fronti/punti.
Livello di sicurezza Garanzia che il sistema di sicurezza si comporti come richiesto.

2.2 Sicurezza nel ICT

Nel campo dell'Informatica, sicurezza significa "sicurezza dell'informazione", cioè "Il grado di resistenza dell'informazione a (o protezione dell'informazione da) un danno". I requisiti fondamentali che se rispettati garantiscono la sicurezza dell'informazione sono la così detta triade CIA:

- **Confidentiality** Confidenzialità, soltanto entità autorizzate (identificate ed autenticate) possono accedere all'informazione (in lettura e/o scrittura).
- **Integrity** Integrità, l'informazione non ha subito modifiche non autorizzate.
- **Availability** L'informazione è disponibile quando richiesta. Il requisito riguarda principalmente i sistemi di stoccaggio e trasmissione dati.

Altri requisiti sono stati aggiunti alla triade CIA e i principali sono:

- **Authenticity** Un sistema informatico che garantisce questo requisito permette di verificare che l'informazione sia autentica, cioè che provenga dalla fonte dalla quale sostiene di provenire.
- **Accountability** Il requisito è che i dati vengano usati in modo chiaro/trasparente e responsabile in accordo alle norme a garanzia degli utenti.[37][38]
- **Non-repudiation** Consiste nel garantire che il mittente di un messaggio non possa successivamente sostenere di non averlo inviato e per contro che il destinatario del messaggio non possa sostenere di non averlo ricevuto.[39][40][41][42]

Principali Modalità di attacco Le principali modalità di attacco che mirano alla violazione dei requisiti di sicurezza dei sistemi informatici sono:

- **Backdoors** Consiste nello sfruttamento di qualsiasi meccanismo presente nel sistema che consenta di bypassare le normali procedure di accesso basate su identificazione e autenticazione. Queste "porte nascoste" possono essere state inserite in modo legittimo per scopi legittimi da chi ha costruito il sistema e poi sfruttate dagli "attaccanti" oppure in qualche modo aggiunte in modo illegittimo una volta ottenuto un accesso.
- **Denial-of-service** Si tratta di attacchi che mirano a rendere non disponibile il sistema agli utenti. Esistono diversi modi per ottenere

questo risultato, dal semplice bloccare l'accesso agli utenti impersonandoli e superando il numero massimo di tentativi con password sbagliate al sovraccaricare un sistema con più richieste di quelle che può soddisfare (interessante per quanto riguarda i dispositivi con scarse risorse computazionali/energetiche l'utilizzo dei loro stessi meccanismi di protezione per mandarli fuori servizio, basta fare leva sui protocolli crittografici ed un dispositivo può essere mandato in DoS facilmente).

- **Direct-access** Una volta ottenuto accesso diretto (di persone o software) ai computer, l'attaccante è in grado di fare qalsiasi cosa con l'hardware, il software e i dati presenti sul dispositivo. Questo è un grosso problema nell'IoT perché la maggior parte dei dispositivi con capacità computazionali lavorerà in ambienti non protetti, dove l'accesso diretto ai dispositivi è semplice.

- **Eavesdropping** Consiste nel "ascoltare" le comunicazioni tra i dispositivi, se per i sistemi tradizionali wired è necessario essere collegati fisicamente al Network, per tutti i sistemi wireless (la tendenza principale nell'IoT) è necessario sviluppare protocolli sicuri per la salvaguardia dei Network accessibili a tutti. Le contromisure usate per prevenire questo tipo di attacco devono tenere in conto anche l'accesso diretto ai dispositivi quindi le tecniche di crittografia tradizionali potrebbero non essere sufficienti (vedi "Side Channel Analysis" [Sez. 2.3.3]).

- **Spoofing** Si tratta di tutte quelle tecniche che mirano ad impersonare un utente diverso da quello che sta operando nel sistema. Un semplice esempio potrebbe essere quello di inviare email cambiando l'indirizzo del mittente con quello della persona che si intende impersonare.

- **Tampering** Il tampering consiste nel modificare un dispositivo affinché si comporti come desiderato dall'attaccante e re-immetterlo nel sistema. Le modifiche possono essere software o hardware e l'effetto ottenuto è quello "cavallo di Troia".

- **Privilege escalation** Tutte quelle tecniche che sfruttando funzionalità e servizi offerti dai sistemi mirano a far guadagnare all'attaccante permessi maggiori di quelli assegnatigli.

- **Clickjacking** Tecnica che mira a sfruttare i privilegi della vittima facendogli compiere operazioni di cui non è al corrente. Se per esempio un utente è loggato su di un Social Network e sta visitando un'altra pagina, l'attaccante proprietario dell'altra pagina può fargli credere che sta cliccando sulla crocetta per chiudere un popup mentre in realtà (attraverso la sovrapposizione di un frame invisibile) sta cliccando su

di un Like nel social Network (potrebbe anche essere una conferma di acquisto o una conferma di reset password).

- **Social engineering** La social engineering consiste nel ottenere informazioni sensibili direttamente dall'utente facendogli credere che chi le chiede è meritevole di fiducia. Nel sistema IoT questo problema coinvolgerà non soltanto gli utenti ma anche le macchine che dovranno decidere autonomamente a chi e cosa comunicare [Sez. 2.3.7]

- **Virus, worms e Trojan** Programmi che una volta installati su di un computer ottengono accesso alle risorse potendone fare qualsiasi cosa, dalla distruzione al furto. Generalmente sono in grado di tentare un infezione alle altre macchine del Network.

- **Spyware e Adware** I primi sono programmi scritti con l'intento di funzionare su di un computer senza che il proprietario se ne accorga rubando e inviando quanti più dati sensibili possibili. I secondi hanno l'intento di visualizzare pubblicità nel sistema infettato.

- **Zero-day attacks, anche chiamati zero-hour attacks** Sono quegli attacchi messi in pratica nel periodo che va dalla scoperta di una vulnerabilità alla messa in campo delle contromisure.

- **Ransomware** Negli ultimi anni si stanno diffondendo questi tipi di virus che attraverso metodi come la crittografia limitano o impediscono l'accesso alle risorse del sistema infettato per poi richiedere un riscatto all'utente che voglia tornare ad avere la disponibilità dei suoi stessi dati.[43]

Esistono diversi database utilizzati per tenere traccia e condividere a scopo di fix le vulnerabilità riguardanti le diverse tecnologie, i principali sono:

- https://nvd.nist.gov/

- http://cve.mitre.org/

Principali Contromisure

- **Riduzione vulnerabilità** Significa trovare i punti deboli dei sistemi e mettere in pratica delle misure per rinforzali. I punti deboli possono essere tecnici come bug o parti progettate con vulnerabilità intrinseche oppure possono appartenere alla componente umana del sistema, per quest'ultima le contromisure da mettere in atto possono consistere nella formazione degli utenti e la sensibilizzazione riguardo agli attacchi ai quali potrebbero essere esposti.

- **Sicuro "by design"** La contromisura madre di tutte le altre è la progettazione dei sistemi tenendo in considerazione tutti i principi sui quali si basa un sistema sicuro. Nella progettazione dei framework per il supporto all'IoT si sta spingendo molto su questo punto.

- **Architetture sicure** L'architettura deve essere definita in modo che sia chiaro quali sono le contromisure adottate e come interagiscono con i sistemi che le adottano al fine di salvaguardare confidenzialità, integrità, disponibilità e responsabilità. Principi fondamentali di architetture sicure sono: la definizione precisa delle relazioni tra i diversi componenti e come essi dipendono uno dall'altro, la valutazione dei rischi, la definizione dei controlli di sicurezza, l'adozione di "buone pratiche" e la standardizzazione dei controlli di sicurezza.

- **Meccanismi di protezione hardware** Quando un dispositivo è fisicamente accessibile, difficilmente le contromisure di sicurezza software possono prevenire efficacemente gli attacchi. Per questo motivo esistono anche metodi hardware per la difesa e si capisce quanto siano fondamentali soprattutto nell'IoT dove l'accessibilità ai dispositivi è molto più semplice che nei sistemi tradizionali. Nuove tecniche stanno nascendo per soddisfare questo livello di sicurezza. [Sez. 2.3.3]

- **Sistemi operativi sicuri** Anche i sistemi operativi utilizzati dai computer devono soddisfare dei requisiti di sicurezza ed esistono standard di valutazione appositi (es ISO/IEC 15408).

- **Identificazione e autenticazione** Sapere chi sta richiedendo l'accesso a una risorsa (identificazione) ed avere la prova che sia effettivamente chi sostiene di essere (autenticazione) è alla base delle politiche di controllo accessi IBAC.

- **Controllo accessi e permessi** Esistono diverse tecniche per la gestione degli accessi ai dispositivi e alle risorse in essi contenute basate su liste, ruoli, attributi, capacità ma nessuna delle soluzioni esistenti sembra soddisfare le necessità dell'IoT dove dispositivi e utenti entrano ed escono continuamente da Network nei quali possono avere privilegi totalmente diversi. [Sez. 2.3.7]

- **Risposte alle violazioni** è l'insieme delle azioni messe in atto in risposta alle violazioni. Consistono principalmente nel rinforzare i punti vulnerabili del sistema, migliorare le capacità di rilevamento violazioni e intentare azioni legali.

- **Anti-virus & Anti-spyware** Programmi in grado di rilevare ed eliminare Virus, worms, Trojan, Spyware e Adware.

- **Firewall** Programmi che monitorano il traffico tra un Network e l'esterno (altro Network o internetwork) filtrando principalmente per IP, tipo di File, URL e contenuti.
- **Intrusion Prevention/Detection Systems** Sono quei software che monitorando il traffico su di un Network o su di un Host e sono in grado di rilevare situazioni anomale, registrarle ed eventualmente bloccare il traffico sospetto.
- **Honeypots & Honeynets** Sono delle risorse/reti deployate per attirare l'attenzione degli attacanti, non contengono informazioni sensibili ma fungono soltanto da esca/distrazione dando il tempo ai sistemi di prevenzione e rilevamento delle intrusioni di fare il loro lavoro e agli addetti del settore di studiare le tecniche degli attaccanti.
- **Criptography** Tecniche di segretazione della comunicazione usate per preservarne la confidenzialità. A seconda della tecnica utilizzata è possibile soddisfare anche principi di integrità, autenticità e non-ripudio.
- **Secure Coding** I software devono essere scritti in modo da non introdurre vulnerabilità (per quanto possibile).
- **Browser security** I browser utilizzati sui computer desktop o sugli smartphone sono una potenziale via d'accesso per gli attaccanti ed anche questi devono essere messi in sicurezza, tanto più perché anche gli smartphone avranno un ruolo importante nell'architettura dei sistemi IoT e presentano già un numero elevato di vulnerabilità.

2.3 IoT security

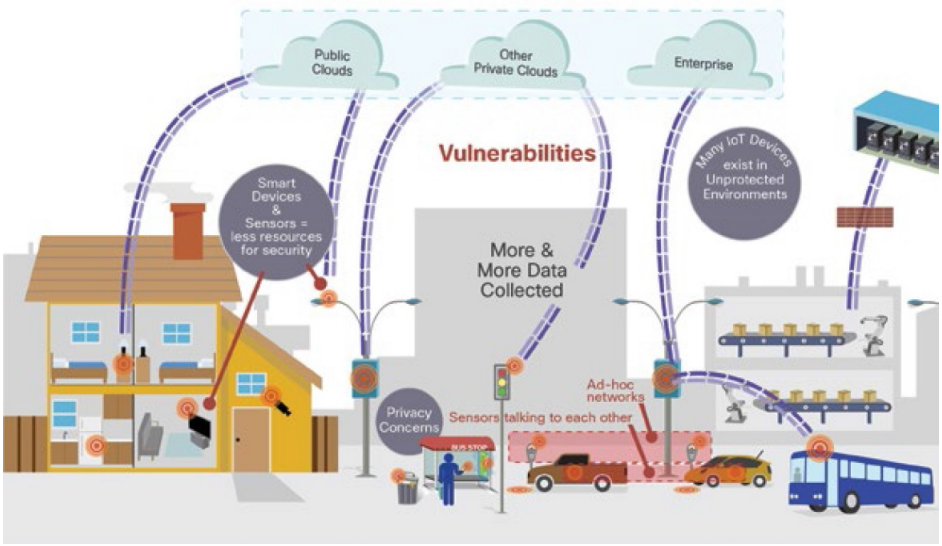


Figura 2.1: IoT Cyber-Physical World [27]

In un sistema esteso come l'IoT, i requisiti di sicurezza devono essere rispettati da diverse tipologie di dispositivi, mezzi di comunicazione, protocolli, metodologie e pratiche. Di seguito sono trattati gli Attacchi e le Vulnerabilità che mettono a rischio i requisiti di sicurezza dei componenti del sistema IoT, sono fornite anche le indicazioni sulle Contromisure adeguate alle minacce (qualora esistenti). L'analisi è suddivisa su ognuno dei layer individuati nelle sezioni "Architettura" [Sez. 1.3.1] e "Network" [Sez. 1.3.2] tenendo conto sia degli studi fatti sulle tecnologie esistenti sia di quelli in corso per le nuove Tecnologie [Sez. 1.3.3]. Non si può parlare di rischi perché questi dipendono dal contesto nel quale viene utilizzato un sistema IoT, per esempio i rischi derivanti dalla violazione della confidenzialità delle informazioni sono diversi se il contesto è uno scenario di guerra o una casa smart. La trattazione quindi cerca di comprendere tutti i possibili attacchi e vulnerabilità delle componenti e relative contromisure senza entrare nel merito della valutazione dei rischi di exploit.

2.3.1 Dispositivi RFD

Le vulnerabilità di questo tipo di dispositivi sono dovute principalmente alle loro scarse (se non nulle) capacità computazionali che li mettono in condizioni di non poter utilizzare contromisure come la crittografia o meccanismi di

autenticazione per mettere in sicurezza i dati che contengono e che comunicano. Le principali modalità di attacco sono l'Accesso Diretto, il Tampering, Eavesdropping delle comunicazioni in chiaro, tutte le tecniche di Side Channel Analysis, lo Spoofing e il DoS.[44][45][46][47] In realtà esistono studi per la messa in sicurezza di questi dispositivi ([48] e standard IEEE 802.15.4) ma l'implementazione dei requisiti individuati fa salire il costo dei dispositivi stessi e di conseguenza fa calare l'interesse del mercato. C'è da dire che questi tipi di dispositivi vengono utilizzati principalmente in ambienti isolati/confinati e quindi possono essere adottate misure di sicurezza indirette e meno costose come per esempio la video-sorveglianza o il controllo accessi fisico [49] il tutto unito a buone prassi di utilizzo come l'evitare di salvare dati sensibili su questi dispositivi.

Device Authentication I dispositivi RFD hanno bisogno di almeno un FFD per scambiare informazioni con il sistema del quale fanno parte e naturalmente anche i dispositivi RFD devono essere identificati e autenticati all'interno del sistema, ma come autenticare un dispositivo con così scarse capacità? una possibile soluzione a riguardo e proposta nel progetto **BUTLER** con un meccanismo di bootstrap tra sensori e Gateway del Wireless Sensor Network basato sulla crittografia ellittica (Elliptic Curve Cryptography).[7] Tuttavia queste metodologie possono essere adottate soltanto su dispositivi con capacità computazionali sufficienti.

2.3.2 Reti PAN

I protocolli più usati dai dispositivi per comunicare a livello di Personal Area Network saranno:

- **6LowPan** Significa "IPv6 over Low-Power Wireless Personal Area Networks" ed è stato sviluppato dal IETF a partire dal RFC 4944 nel rispetto delle specifiche dettate dal IEEE 802.15.4. Considerazioni e possibili implementazioni di misure di sicurezza si trovano a partire dal RFC 6775 e nel Internet-Draft "IPv6 over Low Power WPAN Security Analysis".[50]

- **ZigBee** È uno standard curato dalla ZigBee alliance[51] comprendente i layer Application e Network in accordo agli standard IEEE 802.15.4 ed è stato sviluppato appositamente per favorire la crescita del IoT. Comprende diverse misure di sicurezza[52] ma sono state individuate anche diverse vulnerabilità.[53][54]

- **Bluetooth** Una tecnologia in uso da diversi anni che sicuramente tutti conosciamo, ha subito diverse modifiche e aggiornamenti nel tempo sino alla versione 4.0 che prevede anche modalità di funzionamento a basso consumo energetico. Essendo una tecnologia così utilizzata e

collaudata prevede e dispone di diverse contromisure a salvaguardia della sicurezza.[55][56]

- **NFC** La prima forma di contromisura di cui è dotata questa tecnologia risiede nella sua natura, si tratta infatti della "vicinanza" necessaria ad un dispositivo attaccante per poter comunicare o intercettare la comunicazione tra due dispositivi NFC. Sono inoltre disponibili modalità per la comunicazione crittografata.[57][58][59]

2.3.3 Dispositivi FFD

Le contromisure studiate per garantire la sicurezza nel ICT sino a poco tempo fa non dovevano necessariamente tenere conto delle scarse risorse computazionali ed energetiche dei dispositivi sui quali sarebbero state adottate ma nel contesto dell'IoT, dove i dispositivi che producono e consumano informazioni sono per lo più mobili e alimentati a batteria, devono necessariamente tenerne conto. Sicuramente il metodo più efficace ed adottato per garantire la confidenzialità dell'informazione è la crittografia ed esistono anche implementazioni "ligth" di questa tecnica pensate appositamente per i dispositivi a risorse ristrette. Tuttavia l'attenzione all'aspetto energetico non è sufficiente, esiste un altro grosso problema dovuto alla relativa semplicità con la quale un attaccante può ottenere accesso fisico diretto al dispositivo. Infatti una volta ottenuto l'accesso fisico sono disponibili diverse modalità di estrazione delle chiavi crittografiche attraverso misurazioni e letture dirette sui componenti dei dispositivi o degli output prodotti a fronte di input di test. Queste metodologie vengono chiamate "*Side Channel Analysis*" e come sono stati sviluppati gli attacchi così sono disponibili anche contromisure fisiche e implementazioni software sicure. Per un elenco completo vedere [1] alle sezione 6.3.

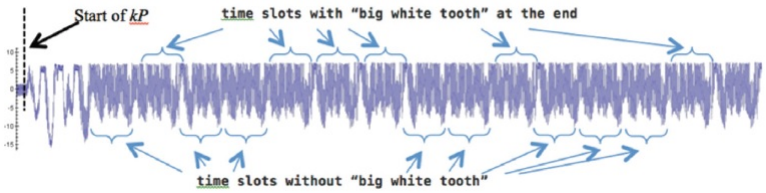


Figura 2.2: Onda ottenuta con metodi di Side Channel Analysis durante l'elaborazione di una chiave crittografica con un algoritmo che non implementa contromusure ala SCA. Nella forma d'onda si nota la differenza durante l'elaborazione di un 1 o di uno 0 della chiave [1]

Tampering Anche questo è un grosso problema nell'IoT, essendo i dispositivi facilmente accessibili è relativamente semplice entrarne in possesso,

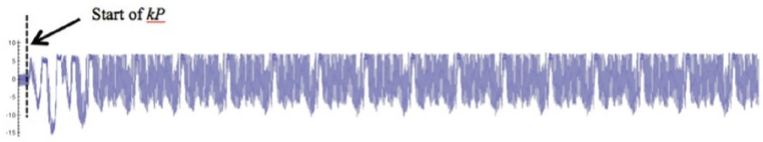


Figura 2.3: Onda ottenuta con metodi di Side Channel Analysis durante l'elaborazione di una chiave crittografica con un algoritmo che implementa contromusure ala SCA [1]

applicavi delle modifiche e re-inserirli nel sistema. Questo tipo di attacco può essere molto dannoso e difficilmente rilevabile in uno scenario dove i dispositivi cambiano Network in continuazione e dove il fatto di scollegarsi e ricollegarsi passa normalmente inosservato.[Sez. 2.3.3] [7]

Malware Attualmente ci si trova nella situazione nella quale i dispositivi hanno capacità computazionali sufficienti per essere soggetti all'attacco di malware ma scarse per supportare meccanismi di difesa (come anti-virus) adeguati.[7]

Mediated access devices Una delle funzioni alle quali dovranno assolvere i dispositivi FFD è quella di "Gateway shield", cioè di controllore locale delle politiche di sicurezza e di privacy, dando garanzie ai dispositivi che i dati da loro prodotti verranno utilizzati seguendo il principio di responsabilità ed eventualmente proteggendoli (come un firewall) da attacchi o minacce provenienti dall'esterno.(Sez. 6.4.1 [1])

2.3.4 Reti LAN

Per quanto riguarda le reti LAN non si prevede lo sviluppo di nuove tecnologie ma si prevede piuttosto un incremento nell'utilizzo delle reti wireless, standard IEEE 802.11. Essendo queste reti largamente testate, studiate e revisionate in diverse versioni dello standard, esistono protocolli di sicurezza sufficientemente robusti per garantirne i requisiti di sicurezza (ovviamente non mancano le vulnerabilità).

Esistono diverse modalità di attacco, da quelle passive come il Wiretapping a quelle attive come il DoS e contromisure che vanno dai sistemi di identificazione e controllo accessi ai sistemi di prevenzione e rilevamento intrusioni. Si può trovare documentazione a riguardo ai seguenti riferimenti: [60][61][62] e molto altro semplicemente cercando in rete. Tuttavia su questo livello, quello sottostante (dei dispositivi FFD) e quelli sovrastanti dovranno essere applicate diverse misure di sicurezza cross-layer specifiche per l'IoT che saranno trattate nella sezione 2.3.7.

Figura 2.4: Communication standards [1]

2.3.5 Reti WAN

Per quanto riguarda le reti WAN, oltre alle "vecchie" tecnologie per le quali sono presenti ampi studi sulla sicurezza, si prevede un incremento dell'utilizzo degli smartphone come punto di accesso e di conseguenza un aumento del traffico nelle reti GSM/EDGE, UMTS/HSPA e loro evoluzioni. Senza dimenticare che questi dispositivi che faranno da punti di accesso sono vulnerabili anche a tutto ciò individuato per i dispositivi RFD e le reti PAN, entriamo del dettaglio delle reti mobili.

L'evoluzione degli smartphone ha portato all'evoluzione delle reti mobili che devono supportare il traffico sempre crescente e il numero di dispositivi connessi. Tuttavia i dispositivi attuali si trovano ad utilizzare ancora i vecchi standard di comunicazione come il 2G imbattendosi nelle loro vulnerabilità. I primi protocolli prevedevano metodi di codifica deboli e alcuni di questi vennero in seguito "banditi" in diversi stati (le comunicazioni criptate con il protocollo A5/2 potevano essere decodificate "al volo", e quelle che utilizzavano l'A5/1 in sole sei ore!). Inoltre il protocollo di comunicazione è deciso dalla stazione radio, quindi un attaccante che simula una stazione radio può facilmente forzare il protocollo più semplice da violare. Nelle successive revisioni sono state adottate contromisure a questi problemi ma comunque esistono ancora numerose vulnerabilità. [63][64][65][66][67]

2.3.6 Cloud

Una volta che i dati arrivano nel così detto Cloud questo eredita tutte le problematiche sulla sicurezza dai dati stessi. A differenza dei dispositivi e dei layer intermedi però questa parte dell'infrastruttura potrebbe non essere

sotto il controllo diretto del proprietario ma fornita da un provider. Come avere garanzia sul rispetto dei requisiti di sicurezza allora?

Computazione verificabile Significa mettere in campo soluzioni in grado di validare la computazione dei dati da parte di entità delle quali non si ha necessariamente fiducia e di rilevare eventualmente computazioni errate/malevoli.(Sez. 6.7.1 [1])

Mantenimento autenticità Consiste nel adottare tecniche per il mantenimento dell'autenticità dell'informazione anche dopo che essa viene processata. Principali modalità utilizzate sono Omomorphic Signatures e Message Authentication Codes.(Sez. 6.7.1 [1])

Garanzia infrastrutture Un cliente deve poter avere garanzie sull'infrastruttura e le misure di sicurezza offerte da un provider di servizi Cloud, tuttavia il provider non può nemmeno svelare i dettagli implementativi sui suoi prodotti a chiunque glielo chieda, è quindi nato di recente il concetto di Graph Signatures dove interviene una terza parte fidata a garantire certe proprietà dei servizi.(Sez. 6.7.2 [1])

Privacy sull'utilizzo dei servizi Il provider deve garantire la privacy sull'utilizzo dei servizi da lui stesso offerti. Infatti l'analisi delle quantità e del tipo dei dati richiesti da un'azienda potrebbe rivelarne le sue politiche di business ovviamente riservate. Metodi a garanzia di questo aspetto della privacy possono essere i metodi di accesso ABAC anonimi.(Sez. 6.7.3 [1])

Sicurezza a lungo termine Visto che non ci si può fidare ciecamente del provider di servizi cloud ne si può assumere che sia immune o sufficientemente "corazzato" contro eventuali attacchi, si potrebbe pensare di inviare dati criptati ma qui si pongono diversi problemi, da quelli riguardanti i DB che potrebbero non supportare il formato dei dati una volta criptati al fatto che il tempo entro il quale un dato criptato rimane al sicuro è finito, cioè il tempo che serve per decriptarlo.(Sez. 6.7.4 e 6.7.5 [1]) Inoltre il tempo si accorcia con l'avvento dei Computer Quantici, problema già preso in considerazione da organizzazioni come l'NSA.[68]

2.3.7 Cross-Layer

In questa sezione sono trattate le problematiche che toccano diversi layer e le relative soluzioni che su diversi layer hanno bisogno di essere implementate.

Fiducia nell'IoT

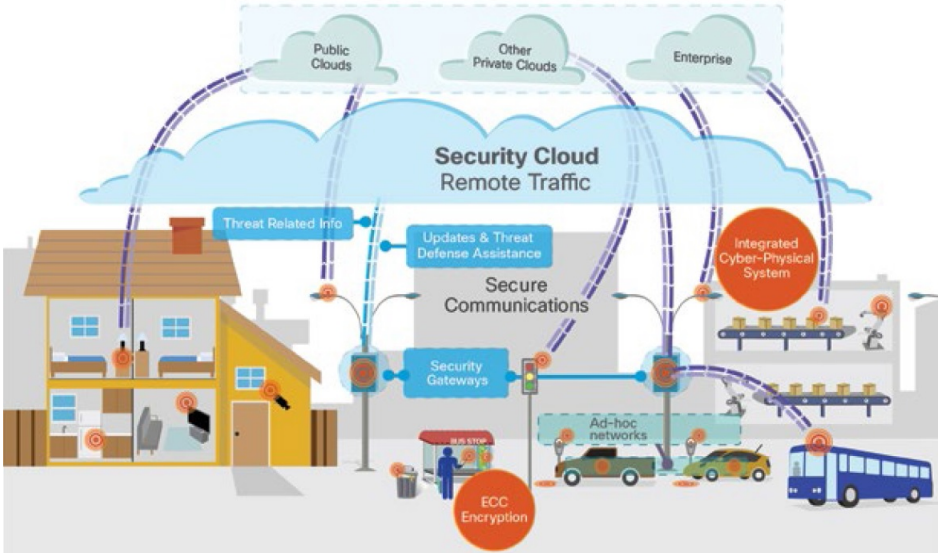


Figura 2.5: Sicurezza multi-strato [27]

Una delle chiavi principali per il successo dell'IoT è la fiducia che gli utenti avranno in questi sistemi. Se nel/per il sistema non sono presenti tecnologie, regolamentazioni e strumenti a garanzia dei requisiti di sicurezza e a prova dell'efficacia delle contromisure, la gran parte degli utenti non sarebbe disposta ad entrare a far parte del sistema stesso. Per questo motivo i dispositivi che saranno chiamati ad interagire tra di loro in maniera autonoma passando attraverso contesti differenti dove spesso "incontreranno" entità sconosciute, avranno bisogno di tecniche e politiche chiare e funzionanti per poter stabilire con *chi* e *come* possono scambiare *quali* informazioni spesso sensibili, si parla infatti di fiducia Uomo-Uomo, Uomo-Macchina e Macchina-Macchina.(Pag. 21 [7])

Trust management framework Perché gli utenti abbiano fiducia in questo nuovo mondo fatto di oggetti smart è dunque necessario che vengano implementate funzionalità avanzate di gestione della sicurezza e di verifica che il sistema rispetti i requisiti prestabiliti.(Sez. 3.8.3 di [1]) Si prevede quindi di integrare nelle entità che fanno parte dell'IoT funzionalità di:

- **Remote control** Le funzionalità di controllo da remoto permettono non solo di localizzare, comunicare e aiutare utenti che magari si trovano in situazioni di pericolo, ma permettono anche di bloccare o resettare dispositivi persi o rubati per eliminare i dati sensibili.(Sez. 2.9.1 di [69])[70]
- **Security updates** I dispositivi devono poter ricevere aggiornamenti sulla sicurezza in modo autonomo, senza la necessità di conferme da

parte del utente e/o di riavviare il dispositivo stesso.

- **Logging** Deve essere possibile tracciare le operazioni fatte dal dispositivo in modo da poter fare controlli di sicurezza in caso vengano riscontrate a posteriori delle anomalie.

- **Strumenti di test** Uno dei metodi per ottenere un minimo di garanzia affinché una tecnologia sia sufficientemente sicura per essere impiegata sul campo consiste nel sottoporla a test. Durante il corso del progetto **SPaCIoS** sono stati sviluppati degli strumenti a supporto di questa fase di sviluppo ed è disponibile un integrazione per il famoso tool di sviluppo Eclipse.(Pag. 59 [7])

Ovviamente anche tutte le altre misure di sicurezza sono in qualche modo funzionali alla fiducia nel IoT.

Identificazione entità

Per quanto riguarda la sicurezza, l'identificazione unita all'autenticazione serve principalmente nei metodi di controllo accessi IBAC. In un ambiente distribuito come l'IoT fatto di utenti, dispositivi, servizi e protocolli diversi si capisce come l'identificazione possa essere un problema complesso. Infatti esistono già molti metodi, da quelli utilizzati nei più piccoli dispositivi come RFID a quelli utilizzati per i server nel Cloud, dalle identità utilizzate nel controllo accessi a quelle utilizzate nel routing dei messaggi.(Pag. 17 [7]) Tuttavia queste diversità non sono necessariamente un problema, se si accetta che le modalità di identificazione possano restare divise in:

- **Numbering** Identificativi fisici degli oggetti (tra cui MAC address);

- **Addressing** Identificativi logici degli oggetti (tra cui indirizzi IP)

- **Naming** Identificativi logici "di secondo livello". Potrebbe essere un esempio lo username.

Esistono già metodi per l'identificazione basati sul Naming che permettono l'interoperabilità di metodi di Numbering e Addressing diversi, inoltre l'utilizzo di pseudonimi invece che di identità "forti" (es. MAC address) garantisce una protezione in più a livello di privacy.(Pag. 67 [7]) Alcuni dei metodi di identificazione che garantiscono interoperabilità attraverso l'utilizzo di pseudonimi si basano su Aouth 2.0, vedi: FaceBook-Connect API e Google Identity Management.

Interessante il progetto **mERA** che fornisce credenziali anonime, quindi un metodo di autenticazione senza identificazione. In pratica chi richiede accesso a delle risorse si identifica (e autentica) soltanto presso un Identity Provider che implementa mERA il quale gli fornisce le credenziali da utilizzare per accedere ad un servizio terzo. Le credenziali non forniscono nessun informazione riguardo l'identità del richiedente accesso e possono essere verificate da chi ha ricevuto la richiesta presso l'Identity Provider per decidere se concederlo o negarlo.(Pag. 69 [7]) Questo metodo potrebbe essere utilizzato in concomitanza a metodi di controllo accessi ABAC.

Controllo accessi

Le informazioni prodotte/contenute nei dispositivi di qualsiasi tipo devono poter essere lette e/o scritte, ma come fa un dispositivo a decidere chi può leggere o scrivere le informazioni in esso contenute? La risposta è l'implementazione di meccanismi di controllo accessi. Controllare l'accesso a un'informazione significa prima stabilire quali requisiti deve avere chi richiede un accesso, poi verificare che ne sia in possesso e solo in questo caso accordarlo. I requisiti si possono raggruppare in tre categorie[71][72]:

1. **IBAC**: Identity-Based Access Control, fanno parte di questa categoria le metodologie che garantiscono un accesso alle risorse basato su requisito di identità del richiedente.

   DAC: Discretionary Access Control, sono i primi metodi sviluppati e attualmente in uso in diversi sistemi operativi, ne fanno parte "Access control matrix", "Access control list" e "Access control capabilities list". Questi metodi non sono adatti a sistemi distribuiti .

   MAC: Mandatory Access Control, sono metodi che forniscono un grado di controllo più specifico e rigido rispetto ai DAC. Sia agli utenti che alle risorse vengono assegnate dall'amministratore determinate classi di sicurezza e solo l'amministratore può modificarle. Questi sistemi sono molto rigidi e complessi nella fase di setup infatti vengono utilizzati in contesti strutturalmente semplici, chiari a priori, con poche risorse e utenti da gestire, per esempio in ambito militare.

2. **RBAC**: Role-Based Access Control, per ovviare allo scarso grado di sicurezza e alla scarsa elasticità in contesti complessi sono stati elaborati i metodi RBAC, dove ad ogni entità viene assegnato uno o più ruoli e ogni ruolo ha uno o più permessi sulle diverse risorse, il requisito che deve possedere il richiedente è dunque di ricoprire uno o più ruoli.

3. **ABAC**: Attribute-Based Access Control, può essere visto come una generalizzazione dei metodi IBAC e RBAC dove l'identità e il ruolo sono casi specifici di ABAC basati appunto sull'attributo identità e ruolo. Nei metodi ABAC non è necessario conoscere a priori l'identità di chi richiederà accesso alle risorse ma è sufficiente stabilire quali attributi debba possedere, sono quindi questi ultimi i requisiti di accesso.

Tuttavia nessuno di questi metodi sembra sufficientemente scalabile e manutenibile nell'ambiente IoT principalmente perché le informazioni necessarie alla valutazione dei requisiti necessari all'accesso sono centralizzate.(Sez. 3.8.3 [1]) Inoltre la maggior parte dei dispositivi che fanno parte dell'IoT sono mobili, si spostano quindi in contesti spaziali e temporali diversi e i requisiti di accesso non possono rimanere gli stessi in posti e momenti diversi. In un determinato posto/momento potrebbe essere consentito l'accesso a certe risorse a chi possiede certi requisiti e in un altro posto/momento il possesso degli stessi potrebbe non essere sufficiente (e viceversa), questo sarebbe un grosso requisito già in un sistema a "contesto statico" dove le relazioni Utente-Macchina e Macchina-Macchina sono per lo più definite a priori, figuriamoci nell'IoT dove le macchine sono tenute ad applicare autonomamente le politiche di controllo accessi. Si capisce quanto questo requisito possa essere una sfida non di poco conto.(Pag. 15 [7]) Di seguito principi, necessità e soluzioni trovate.

Least Privilege Principle & Fine-Grained Authorization Il primo è il principio fondamentale secondo il quale ad un utente (in questo caso si può parlare di entità in generale) deve essere assegnato soltanto il minimo insieme di permessi necessari a portare a termine le operazioni che deve svolgere. Il secondo consiste nel definire relazioni strette e puntuali tra risorse e entità autorizzate ad accedervi. L'insieme di questi principi è un arma in più per la prevenzione di attacchi basati sull'eccesso di autorizzazioni [73] e sulla Privilege escalation [74]. Tuttavia più sono rispettati rigidamente questi principi più sono rigidi e difficili da gestire i sistemi che ne fanno uso (vedi modelli MAC).

Context awareness La discriminante sulla quale decidere chi deve essere in grado di fare cosa sembra quindi essere il contesto, dove per contesto si intente l'*insieme di informazioni che descrivono la situazione, il luogo e il momento* nel quale si trova ad operare l'entità in questione. Un modello che implementa il controllo accessi basato sulla consapevolezza del contesto appositamente studiato per l'IoT è stato sviluppato nel progetto **iCORE**, si chiama SecKit e permette di gestire anche il deploy dinamico delle politiche di sicurezza.[75](Sez. 6.6 [1]) Da notare che questa soluzione fa affidamento su politiche di accesso IBAC e RBAC con le problematiche di controllo

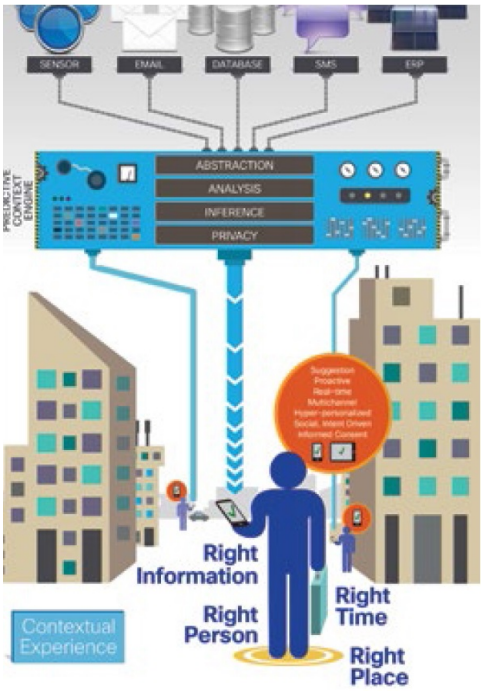


Figura 2.6: Consapevolezza del contesto [27]

centralizzato derivanti. Un altro approccio basato sul cosiddetto "Osmotic context Management" è stato sviluppato nel progetto **OSMOSE**(Sez. 5.5 [1])[76]

Trust negotiation Protocolli nati per i sistemi computazionali distribuiti e che sulla base di *catene di politiche di fiducia* permettono a due parti di stabilire il minimo livello di fiducia richiesto per accedere alle risorse.(Sez. 2.9.1 di [69])[77] L'obiettivo è quello di permettere a entità sconosciute di negoziare autonomamente le credenziali per accedere alle risorse sulla base dei requisiti di fiducia avanzati da entrambe le parti (per esempio il client potrebbe avere come requisiti la confidenzialità e il server il pagamento di una corrispettivo).[78] Questo modello di controllo accessi è totalmente decentralizzato e garantisce una grande autonomia ai dispositivi.

Reputazione Nel progetto **COMPOSE** è stato preso in considerazione un'altro parametro per l'implemetazione del C.A., la *reputazione*. Attraverso l'elaborazione di informazioni come popolarità, feedback ricevuti, qualità dei servizi offerti, garanzie di sicurezza offerte ecc. riguardanti una data entità, le viene accordato un certo grado di fiducia utilizzato per discriminare a quali risorse può accedere.(Pag. 67 [7])

Capability-Based Access Control Può essere visto come un caso specifico di ABAC dove l'attributo che garantisce accesso alla risorsa è la "Capability". Il sistema è stato sviluppato nel progetto **IoT@Work** rispettando i principi di Least Privilege Principle e Fine-Grained Authorization probabilmente perché studiato per contesti industriali e di automazione. Tra le altre cose permette la delegazione dinamica delle capability.[79][1]

Privacy By Design

Ovviamente sono necessari anche meccanismi di prevenzione della privacy degli utenti, infatti i dispositivi non possono essere lasciati liberi di raccogliere e trasmettere dati senza alcun accorgimento che prevenga una diffusione non controllata di informazioni, informazioni attraverso la correlazione delle quali si possa risalire ad aspetti della vita privata degli utenti. Riguardo questo tema sono stati individuati i seguenti principi e soluzioni.

Minimizzazione raccolta e diffusione dati È il principio fondamentale che semplifica qualsiasi altro accorgimento successivo. La quantità di dati raccolta deve essere piccola il più possibile, devono essere raccolti soltanto i dati indispensabili a fornire i servizi che si stanno sviluppando, ed è responsabilità dei progettisti individuare questo insieme minimo. Inoltre i dati raccolti devono essere trasmessi il minor numero di volte possibile e restare il "più locali possibile".(Sez. 6.4.4 [1]) Questo obiettivo può essere raggiunto con accorgimenti adeguati durante la fase di Fog & Edge Computing. L'applicazione di questo principio ha come effetto secondario anche il miglioramento delle prestazioni del sistema.

Anonimizzazione dati Una volta minimizzata la quantità di dati raccolti si rende necessario poterli anonimizzare, cioè scollegare l'informazione dal dispositivo/entita/utente che l'ha prodotta o il quale riguarda. Questa funzionalità è messa a disposizione attraverso l'utilizzo di pseudonimi dal SecKit [80] quindi può essere implementata da tutti i dispositivi classificati FFD.

Data re-identification La raccolta di dati provenienti da diversi contesti permetterebbe la ricostruzione di profili precisi e dettagliati sulla vita privata degli utenti, il problema sembrerebbe risolto con l'anonimizzazione dei dati ma in realtà esistono algoritmi per la re-identificazione degli utenti/entità che li hanno prodotti.[81][82]. Una possibile soluzione sembra essere l'aumentare volutamente la quantità di dati producendone di falsi ma simili agli originali per abbassare le percentuali di accuratezza nella re-identificazione.[83]

Prevenzione Traffic Analysis Per prevenire attacchi alla privacy basati sull'analisi del traffico dati si rende necessario nascondere le identità delle parti in comunicazione e il fatto stesso che esse stiano comunicando. L'identità delle parti può essere dedotta attraverso analisi "Brute force" dei metadati utilizzati nei protocolli di comunicazione oppure monitorando alcune proprietà dei messaggi quali: codifica, grandezza, tempistiche, numero dei messaggi ecc.. attraverso l'analisi di queste informazioni è possibile risalire agli attori della comunicazione. Alcune tecniche utilizzate per far fronte a queste minacce sono: catene di proxy (tipo TOR), cambio di codifica messaggi, Messaggi a grandezza fissa, Random delayed messages, ricezione e invio di un numero standard di messaggi ecc.. (Sez. 6.5 [1])

Deploy sicuro

La fase di setup/deploy è uno dei momenti più delicati perché in questa fase vengono impostate/scambiate le configurazioni a protezione della sicurezza come le chiavi utilizzate per la crittografia. Un attaccante potrebbe interferire modificando le informazioni scambiate in questa fase oppure intercettarle rendendo totalmente inefficace qualsiasi meccanismo adottato. È quindi necessario prevedere modalità di bootstrap sicuro del sistema che tengano conto anche delle scarse risorse energetiche e computazionali dei dispositivi RFD. Il problema riguarda più che altro questi dispositivi perché sono quelli più esposti all'accesso diretto degli attaccanti sui quali quindi è sconveniente utilizzare chiavi statiche preimpostate.

Cofigurazione autonoma Per garantire la sicurezza nella fase di setup della comunicazione end-to-end sono stati sviluppati meccanismi di scambio autonomo delle chiavi tra dispositivi "che non si conoscono a priori"[84] e, nel progetto **RERUM**, meccanismi di produzione autonoma delle chiavi basati sul "Channel Sensing"(Pag. 66 [7])

Capitolo 3

Questioni etiche e sociali

Lo sviluppo tecnico dell'IoT corre molto più velocemente dell'analisi sui suoi possibili impatti socio economici e sulle questioni etiche introdotte da un sistema così esteso e invasivo. Basti pensare ai cambiamenti introdotti nella società dai computer e da internet negli ultimi anni per rendesi conto di quanto potrebbe mutare la nostra realtà nel prossimo decennio. L'analisi di quali potrebbero essere le implicazioni sociali è infatti tutt'altro che semplice data la complessità dei casi d'uso e l'opacità delle intenzioni delle aziende che già stanno sviluppando e mettendo in produzione sistemi IoT. Le possibilità di miglioramento di molti degli aspetti delle nostre vite sono tanti, come l'ottimizzazione dei consumi energetici, ma sono tante anche le preoccupazioni su chi e come utilizzerà i dati necessari a fornire questi servizi. Quali effetti avrà inoltre sull'economia e sul lavoro? e sulla politica e le amministrazioni?

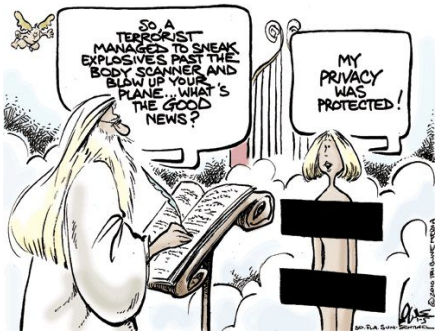
3.1 Fiducia

L'introduzione di dispositivi intelligenti in grado di prendere decisioni autonome, decisioni basate su regole programmate dai fornitori dei dispositivi stessi, presuppone un grande livello di fiducia da parte degli utenti nei confronti dei fornitori di queste tecnologie. I dispositivi sono infatti in grado di ricevere e inviare dati da/a entità sconosciute in modo dinamico, dati che la maggior parte delle volte non sapremo come e da chi verranno utilizzati per fornire quali servizi. [85] Allo stesso tempo i fornitori dei servizi che andranno ad implementare sistemi IoT dovranno avere fiducia nei loro fornitori di tecnologie e servizi Cloud, ma anche che i sistemi vengano utilizzati nel modo corretto e non subiscano modifiche malevole. Alcune soluzioni per garantire questi rapporti di fiducia reciproca sono stati individuati nella sezione 2.3.7 e sono argomento di [77]. Naturalmente tutte le misure di sicurezza dovrebbero concorrere a garantire i rapporti di fiducia tra le parti

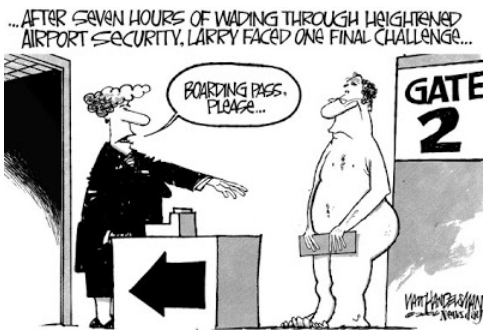
ma certi aspetti sono fuori dal dominio tecnologico e fanno parte di quello culturale e legislativo dei diversi popoli.

3.2 Privacy vs Security

Forse la privacy è l'aspetto più sentito e più trattato quando si parla di informazione, infatti è tenuto in grossa considerazione nella progettazione dei sistemi IoT. Basti pensare a tutti i problemi e rinvii subiti dal progetto "Smart Meter Programme" in Gran Bretagna che aveva come scopo quello di migliorare i consumi energetici nazionali per allinearsi alla direttiva europea del 1996. La necessità di installare dei sensori nelle case provocò un putiferio mediatico secondo il quale l'analisi dei dati sui consumi avrebbe potuto rivelare abitudini personali delle famiglie e persino quali film avessero guardato in TV.[85] Tralasciando il perché qualcuno voglia tenere segreto quali film guardi alla TV e quali giorni delle settimana faccia il bucato, è piuttosto evidente il bisogno di privacy degli utenti. Per questo motivo, come abbiamo visto nella sezione 2.3.7, la privacy è tenuta in grande considerazione nella progettazione del IoT, si cerca di garantire l'anonimizzazione dei dati raccolti dai sensori, l'anonimizzazzione del traffico dati, la confidenzialità della comunicazione ad ogni livello, la non re-identificabilità dei dati nel Fog/Cloud. Ma un tale livello di privacy è sempre un bene o esistono dei casi nei quali potrebbe diventare un male? Quali potrebbero essere gli strumenti a sorveglianza di questa tecnologia se viene garantito un tale livello di privacy? queste sono domande che probabilmente vale la pena porsi prima di creare uno strumento talmente potente.[7]



(a) Privacy airport



(b) Security airport

3.3 Economia e Lavoro

Come trattato nella sezione 1.2 il settore con un maggiore impatto/adozione di tecnologie IoT sarà quello industriale dove già computer e robot hanno

avuto e stanno avendo un gran successo. Ma quali conseguenze avrà l'adozione di queste nuove tecnologie su questo settore? Presumibilmente vi sarà uno spostamento delle raccolta di informazioni da "manuale" a digitale attraverso i sensori e una maggiore centralizzazione della fase di decision-making. Anche il lavoro verrà ottimizzato in tempi e consumi di energie probabilmente anche con un maggiore utilizzo di robot. I lavoratori avranno impieghi sempre più di responsabilità e controllo sull'operato delle things, necessiteranno quindi di una formazione superiore (e qui si potrebbero aprire dibattiti sul digital divide implicito nei lavoratori più "anziani"). Inoltre il fatto di far parte di un sistema IoT del quale vengono analizzati tutti i dati potrebbe far sentire i lavoratori come "sorvegliati" sul lavoro che svolgono, ma questi dati d'altronde potrebbero essere utilizzati anche per ottenere maggiori garanzie di sicurezza sul lavoro.[85]

3.4 Delegazione autonomia

La tendenza in un mondo dove oggetti e persone sono strettamente connessi sembra essere quella di una sempre maggiore delegazione di certe attività agli oggetti sempre più smart. Questa delegazione comprende anche la capacità di svolgere certi lavori che stanno ormai passando "in mano" alle macchine. Gli utenti più "colpiti" da questa problematica saranno le nuove generazioni che nascendo con l'IoT vi faranno affidamento come se fosse una cosa scontata/naturale. Si potrebbe pensare "certo come ora noi dipendiamo da automobili ed elettricità e i nostri avi potevano farne a meno", ma vi è una grossa differenza, gli oggetti smart sono progettati per *agire autonomamente al nostro posto* (non su nostra richiesta) in base alle specifiche decise dai costruttori.[7]

3.5 Influenza sociale

Da sempre il potere va a braccetto con la raccolta e gestione dell'informazione, si capisce dunque quanto l'IoT possa essere allettante anche per il campo della politica. C'è chi sostiene che l'IoT sarà il più grande strumento politico mai creato che cambierà non solo il ruolo degli elettori ma anche come i politici analizzano e intervengono nei diversi paesi. Se fino ad ora i politici hanno ascoltato, discusso con rappresentanti e fatto sondaggi per analizzare i desideri degli elettori, con l'avvento dell'internet delle cose potranno avvalersi dell'analisi dei dati comportamentali raccolti dalle things, dati non affetti da falsità (volontarie e non) e deformazioni ideologie della realtà. Questo strumento potrà essere utilizzato tuttavia non soltanto per raccogliere informazioni sui bisogni delle persone ma anche dai lobbisti per influenzare gli elettori come ha fatto Uber che in Cina ha ordinato ai tassisti di stare lontani dalle proteste minacciando i contravventori di vedere il loro

contratto revocato, questa azione anche se può sembrare soltanto di business ha avuto l'effetto di sfavorire i chi volesse partecipare alle proteste per la rifocrma del governo.[86]

3.6 Isolamento socio-culturale

Le tecnologie informatiche possono essere uno strumento utile ad avvicinare persone, culture, enti e organizzazioni, fornendo un collegamento in più, da aggiungere/affiancare a quello reale/fisico, tuttavia se fraintese o mal utilizzate possono diventare motivo di isolamento. Esistono principalmente due tipi di isolamento causato dal ICT, l'isolamento *nel* mondo virtuale e l'isolamento *dal* mondo virtuale. Al primo tipo sono soggetti individui con tendenze "innate" all'isolamento che trovano uno strumento in grado di amplificarle dando un falso senso di "non isolamento", quello che avviene in realtà è l'isolamento dal mondo reale che lascia il posto alla connessione ad un mondo virtuale (quindi finto per definizione). L'isolamento dal mondo virtuale è una problematica totalmente diversa e riguarda tutte le persone che non possono (mancanza di strumenti), non riescono (per esempio per motivi di età) o non hanno interesse ad entrare/connettersi al mondo virtuale. Questo secondo tipo di isolamento è in grado di causare problematiche sociali ed economiche ben più gravi del primo come l'accrescimento delle differenze socio economiche tra paesi più o meno informatizzati o semplicemente tra persone "digitalizzate" e non.[1][7] Si chiama "Digital Divide" ed è stato già riscontrato e analizzato per quanto riguarda le tecnologie già in uso.

Bibliografia

[1] O. Vermesan and P. Friess, *Building the Hyperconnected Society*. 2015. Online at: http://www.internet-of-things-research.eu/pdf/Building_the_Hyperconnected_Society_IERC_2015_Cluster_eBook_978-87-93237-98-8_P_Web.pdf.

[2] Wikipedia, "Kevin ashton," 2016. Online at: https://en.wikipedia.org/wiki/Kevin_Ashton.

[3] L. R. LLC, "An introduction to the internet of things (iot)," 2013. Online at: http://www.cisco.com/c/dam/en_us/solutions/trends/iot/introduction_to_IoT_november.pdf.

[4] K. Ashton, "That 'internet of things' thing," 2009. Online at: http://www.rfidjournal.com/articles/view?4986.

[5] Postscapes, "A brief history of the internet of things," 2016. Online at: http://postscapes.com/internet-of-things-history.

[6] Google, "Google trends," 2016. Online at: http://www.google.com/trends/explore?hl=en-US#q=internet+of+things.

[7] O. Vermesan, P. Friess, and et al., "Internet of things - iot governance, privacy and security issues," 2015. Online at: http://www.internet-of-things-research.eu/pdf/IERC_Position_Paper_IoT_Governance_Privacy_Security_Final.pdf.

[8] S. Aguzzi, D. Bradshaw, M. Canning, M. Cansfield, P. Carter, G. C. adn Sergio Gusmeroli, G. Micheletti, D. Rotondi, and R. Stevens, "Definition of a research and innovation policy leveraging cloud computing and iot combination," 2013. Online at: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=9472.

[9] G. Inc., "Gartner identifies the top 10 strategic technology trends for 2016," 2015. Online at: http://www.gartner.com/newsroom/id/3143521.

[10] I. T. Union, "Itu-t rec. y.2060 (06/2012) overview of the internet of things," 2012. Online at: https://www.itu.int/rec/T-REC-Y.2060-201206-I.

[11] O.vermesan, P. Friess, P.Guillemin, S. Gusmeroli, and et al., *Internet of Things Strategic Research and Innovation Agenda*. 2013. Online at: https://books.google.it/books?id=Eug-RvslW30C&lpg=PR4&ots=3Tw5vFeBvw&dq=isbn%20978-87-92329-67-7%20Global%20Technological%20and%20Societal%20Trends&hl=it&pg=PP1#v=onepage&q&f=false.

[12] J.-M. Chung, "Iot architecture," 2015. Online at: https://www.coursera.org/learn/iot-augmented-reality-technologies/lecture/8ZlnC/iot-architecture.

[13] J.-M. Chung, "Iot networks," 2015. Online at: https://www.coursera.org/learn/iot-augmented-reality-technologies/lecture/M0lLQ/iot-networks.

[14] Wikipedia, "Radio-frequency identification," 2016. Online at: https://en.wikipedia.org/wiki/Radio-frequency_identification.

[15] Wikipedia, "Near field communication," 2016. Online at: https://en.wikipedia.org/wiki/Near_field_communication.

[16] Wikipedia, "Zigbee," 2016. Online at: https://en.wikipedia.org/wiki/ZigBee.

[17] Wikipedia, "6lowpan," 2016. Online at: https://en.wikipedia.org/wiki/6LoWPAN.

[18] S. E. Deering and et al., "Internet protocol, version 6 (ipv6) specification," 1998. Online at: https://tools.ietf.org/html/rfc2460.

[19] Wikipedia, "Gsm," 2016. Online at: https://en.wikipedia.org/wiki/GSM.

[20] Wikipedia, "Universal mobile telecommunications system," 2016. Online at: https://en.wikipedia.org/wiki/Universal_Mobile_Telecommunications_System.

[21] Wikipedia, "Lte (telecommunication)," 2016. Online at: https://en.wikipedia.org/wiki/LTE_(telecommunication).

[22] Wikipedia, "Lte advanced," 2016. Online at: https://en.wikipedia.org/wiki/LTE_Advanced.

[23] F. Semiconductor, "What the internet of things (iot) needs to become a reality - white paper," 2014. Online at: http://www.nxp.com/files/32bit/doc/white_paper/INTOTHNGSWP.pdf.

[24] Wikipedia, "Ieee 802.15.4," 2016. Online at: https://en.wikipedia.org/wiki/IEEE_802.15.4.

[25] J.-M. Chung, "Iot technologies," 2015. Online at: https://www.coursera.org/learn/iot-augmented-reality-technologies/lecture/Cebzu/iot-technologies.

[26] R. van der Meulen, "Gartner says the internet of things will drive device and user relationship requirements in 20 percent of new iam implementations by 2016," 2014. Online at: http://www.gartner.com/newsroom/id/2944719.

[27] S. Monterde, "Technology radar," 2014. Online at: https://techradar.cisco.com/technology/securing-the-internet-of-things.

[28] Google, "Google cloud platform," 2016. Online at: https://cloud.google.com/solutions/iot/.

[29] Google, "Brillo," 2016. Online at: https://developers.google.com/brillo/.

[30] Google, "Weave," 2016. Online at: https://developers.google.com/weave/.

[31] Microsoft, "Internet delle cose," 2016. Online at: https://www.microsoft.com/it-it/server-cloud/internet-of-things/azure-iot-suite.aspx.

[32] Apple, "Homekit," 2016. Online at: https://developer.apple.com/homekit/.

[33] Samsung, "Smartthings," 2016. Online at: https://www.smartthings.com/.

[34] Samsung, "Artik," 2016. Online at: https://www.artik.io/.

[35] Cisco, "Internet of things," 2016. Online at: http://www.cisco.com/c/en/us/solutions/internet-of-things/overview.html.

[36] Wikipedia, "Security," 2015. Online at: https://en.wikipedia.org/wiki/Security.

[37] T. I. A. Foundation, "The information accountability foundation," 2016. Online at: http://informationaccountability.org/.

[38] D. J. Weitzner, H. Abelson, T. Berners-Lee, J. Feigenbaum, J. Hendler, and G. J. Sussman, "Information accountability," 2008. Online at: http://dig.csail.mit.edu/2008/06/info-accountability-cacm-weitzner.pdf.

[39] V. Beal, "nonrepudiation," 2016. Online at: http://www.webopedia.com/TERM/N/nonrepudiation.html.

[40] Techopedia, "Nonrepudiation," 2016. Online at: https://www.techopedia.com/definition/4031/nonrepudiation.

[41] ommission for the Protection of Privacy, "Non-repudiation (information security)," 2016. Online at: https://www.privacycommission.be/en/glossary/non-repudiation.

[42] M. Rouse, "nonrepudiation," 2008. Online at: http://searchsecurity.techtarget.com/definition/nonrepudiation.

[43] Cisco, "Report semestrale sulla sicurezza," 2015. Online at: http://www.cisco.com/web/offers/lp/2015-midyear-security-report/index.html?keycode=000854765.

[44] ThingMagic, "Rfid security issues - generation2 security," 0000. Online at: http://www.thingmagic.com/index.php/rfid-security-issues.

[45] D. Suprina, "Security risks with rfid," 2015. Online at: http://www.rfidjournal.com/articles/view?1564.

[46] T. G. of the Hong Kong Special Administrative Region, "Rfid security," 2008. Online at: http://www.infosec.gov.hk/english/technical/files/rfid.pdf.

[47] NearFieldCommunication.org, "Security concerns with nfc technology," 2016. Online at: http://www.nearfieldcommunication.org/nfc-security.html.

[48] B. R. Ray, M. Chowdhury, and J. Abawajy, "Critical analysis and comparative study of security for networked rfid systems," 2013. Online at: http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=6598466.

[49] Cisco, "Cisco iot system," 2015. Online at: http://www.cisco.com/c/dam/en/us/products/collateral/se/internet-of-things/brochure-c02-734481.pdf.

[50] S. Park, S. Electronics, K. Kim, A. University, W. H. (Ed.), S. Chakrabarti, Ericsson, J. Laganier, and Juniper, "Ipv6 over low power wpan

security analysis," 2011. Online at: https://tools.ietf.org/html/draft-daniel-6lowpan-security-analysis-05.

[51] Z. Alliance, "Zigbee," 2016. Online at: http://www.zigbee.org/.

[52] Z. Alliance, "Zigbee 3.0 – the open, global standard for the internet of things," 2014. Online at: http://www.zigbee.org/?wpdmdl=2176.

[53] T. Zillner, "Zigbee exploited the good, the bad and the ugly," 2015. Online at: https://www.blackhat.com/docs/us-15/materials/us-15-Zillner-ZigBee-Exploited-The-Good-The-Bad-And-The-Ugly-wp.pdf.

[54] B. Bowers., "Zigbee wireless security: A new age penetration tester's toolkit," 2012. Online at: http://www.ciscopress.com/articles/article.asp?p=1823368&seqNum=4.

[55] S. S and S. D. K. A, "Analysis of bluetooth threats and v4.0 security features," 2012. Online at: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6179149.

[56] J. Padgette, K. Scarfone, and L. Chen, "Guide to bluetooth security," 2012. Online at: http://csrc.nist.gov/publications/nistpubs/800-121-rev1/sp800-121_rev1.pdf.

[57] E. Haselsteiner and K. Breitfuß, "Security in near field communication (nfc)," 0000. Online at: http://events.iaik.tugraz.at/RFIDSec06/Program/papers/002%20-%20Security%20in%20NFC.pdf.

[58] A. Alzahrani, A. Alqhtani, H. Elmiligi, F. Gebali, , and M. S. Yasein, "Nfc security analysis and vulnerabilities in healthcare applications," 2013. Online at: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6625493.

[59] W. H. Wei Fan, Z. Zhang, Y. Wang, and D. Sun, "A near field communication(nfc) security model based on osi reference model," 2015. Online at: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7345433.

[60] Wikipedia, "Wireless security," 2016. Online at: https://en.wikipedia.org/wiki/Wireless_security.

[61] CISCO, "Wireless and network security integration solution design guide," 2008. Online at: http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Mobility/secwlandg20/sw2dg/ch3_2_SPMb.html.

[62] K. Scarfone and P. Mell, "Guide to intrusion detection and prevention systems (idps)," 2007. Online at: http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf.

[63] M. Pannu, R. Bird, B. Gill, and K. Patel, "Investigating vulnerabilities in gsm security," 2015. Online at: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7344480.

[64] J. Cao, M. M. H. Li, Y. Zhang, and Z. Luo, "A survey on security aspects for lte and lte-a networks," 2014. Online at: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6506141.

[65] F. Imran and M. Hussain, "A review of salient security aspects of the universal mobile telecommunication system (umts)," 2011. Online at: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5983559&tag=1.

[66] C. Blanchard, "Security for the third generation (3g) mobile system." Online at: http://www.uniroma2.it/didattica/netsec/deposito/3g_umts_security.pdf.

[67] Wikipedia, "Mobile security," 2016. Online at: https://en.wikipedia.org/wiki/Mobile_security.

[68] NSA, "Cryptography today," 2015. Online at: https://www.nsa.gov/ia/programs/suiteb_cryptography/.

[69] O. Vermesan and P. Friess, *Converging Technologies for smart Environments and Integrated Ecosystems*. 2013. Online at: http://www.internet-of-things-research.eu/pdf/Converging_Technologies_for_Smart_Environments_and_Integrated_Ecosystems_IERC_Book_Open_Access_2013.pdf.

[70] Google, "Come fare squillare, bloccare o resettare da remoto un dispositivo perso," 2016. Online at: https://support.google.com/accounts/answer/6160500.

[71] B. Qing-hai and Z. Ying, "Study on the access control model in information security," 2011. Online at: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6037079.

[72] V. C. H. andDavid Ferraiolo andRick Kuhn andAdam Schnitzer andKenneth Sandlin andRobert Miller andKaren Scarfone, "Guide to attribute based access control (abac) definition and considerations," 2014. Online at: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-162.pdf.

[73] H. Wang, L. Liu, and W. Tian, "An authorization model of quantitative analysis of the least privilege," 2012. Online at: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6528642.

[74] Wikipedia, "Privilege escalation," 2016. Online at: https://en.wikipedia.org/wiki/Privilege_escalation.

[75] R. Neisse, I. N. Fovino, G. Baldini, V. S. andPanagiotis Vlacheas, and R. Giaffreda, "A model-based security toolkit for the internet of things," 2014. Online at: http://ricardo.neisse.name/images/publications/neisse-ares2014.pdf.

[76] OSMOSE, "Osmose," 2016. Online at: http://demos.txt.it:8097/.

[77] S. Sicari, A. Rizzardi, L. Grieco, and A. Coen-Porisini, "Security, privacy and trust in internet of things: The road ahead," 2015. Online at: http://ac.els-cdn.com/S1389128614003971/1-s2.0-S1389128614003971-main.pdf?_tid=1cdf2d7e-e3c9-11e5-ac9f-00000aab0f6b&acdnat=1457289041_01cc3c584027725d459cf6d51c50b076.

[78] A. Klenk, G. Carle, B. Radier, and M. Salaun, "Secure stateless trust negotiation," 2009. Online at: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5161674.

[79] IoT@Work, "Internet of things at work," 2013. Online at: https://www.iot-at-work.eu/.

[80] D. O. Vermesan and D. P. Friess, *Internet of Things Applications - From Research and Innovation to Market Deployment*. 2014. Online at: http://www.internet-of-things-research.eu/pdf/IoT-From%20Research%20and%20Innovation%20to%20Market%20Deployment_IERC_Cluster_eBook_978-87-93102-95-8_P.pdf.

[81] A. R. L. Singh, E. Porter, and F. Nagle, "Exploring re-identification risks in public domains," 2012. Online at: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6297917.

[82] A. Cecaj and M. M. N. Bicocchi, "Re-identification of anonymized cdr datasets using social network data," 2012. Online at: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6815210.

[83] N. McLaughlin, J. M. D. Rincon, and P. Miller, "Data-augmentation for reducing dataset bias in person re-identification," 2015. Online at: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7301739.

[84] P. Porambage, A. Braekeny, P. Kumar, A. Gurtovz, and M. Ylianttila, "Proxy-based end-to-end key establishment protocol for the internet of things," 2015. Online at: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7247583.

[85] J. Crump and I. Brown, "The societal impact of the internet of things," 2013. Online at: https://www.bcs.org/upload/pdf/societal-impact-report-feb13.pdf.

[86] P. Howard, "Politics won't know what hit it. the internet of things is poised to change democracy itself.," 2015. Online at: http://www.politico.com/agenda/story/2015/06/philip-howard-on-iot-transformation-000099.

Elenco delle figure