Alma Mater Studiorum · Università di Bologna

SCUOLA DI SCIENZE

Laurea Magistrale in Informatica

TITOLO DELLA TESI

Relatore:
Chiar.mo Prof.
Marco Di Felice

Presentata da:
Daniele Rossi

Sessione III
Anno Accademico 2018/2019

Questa è la Dedica*:*
ognuno può scrivere quello che vuole,
anche nulla . . .

Indice

Elenco delle figure

Elenco dei listati di codice

Introduzione

Questa è l'introduzione.

Parte 1

Stato dell'arte

Capitolo 1

Internet of Things

Con il termine Internet of Things (IoT) si indica un paradigma in cui la rete Internet viene integrata con oggetti fisici. Nell'IoT, la rete Internet non è più una semplice collezione di contenuti multimediali, ma viene estesa al mondo fisico, real-time, trasformandosi in una rete di oggetti di ogni genere e dimensione: auto, smartphone, videocamere, applicazioni per la casa, giocattoli, strumenti medici, sistemi industriali, animali, persone, edifici ecc. Tutti questi oggetti sono connessi tra loro e comunicano scambiandosi informazioni. Attraverso l'integrazione con la rete Internet, essi vengono "potenziati", acquisiscono intelligenza e nuove funzionalità così da essere in grado di svolgere nuovi compiti. Gli oggetti appartenenti a questa nuova classe prendono il nome di *smart things* o semplicemente *Things*.

Una *smart thing*, quindi, è un oggetto fisico che viene potenziato digitalmente tramite una o più delle seguenti caratteristiche:

- sensori (temperatura, luce, movimento, ecc.)
- attuatori (schermi, motori, ecc.)
- computazione (capacità di eseguire programmi e logica)
- interfacce di comunicazione (cablate o wireless)

Unendo le parole e i concetti di "Internet" e "Things", si ottiene la nuova tipologia di rete Internet globale costituita da oggetti fisici in grado di fare sensing, attuare azioni, eseguire calcoli, comunicare e scambiare informazioni, che è proprio l'Internet of Things.

Il concetto dell'Internet of Things come lo conosciamo oggi è il risultato di un lungo processo di raffinazione e espansione che è stato portato avanti nel corso di decenni.

La prima comparsa del termine risale al 1999 e la sua paternità è da attribuire a Kevin Ashton, cofondatore e direttore esecutivo di Auto-ID Center (consorzio di ricerca con sede al Massachusetts Institute of Technology), il quale, all'epoca, si riferiva solo ed esclusivamente a quei dispositivi connessi che potevano essere identificati in modo univoco tramite la tecnologia Radio-Frequency IDentification (RFID).

Con il passare del tempo, grazie anche allo sviluppo delle reti di sensori wireless (WSNs), le capacità sensoristiche e computazionali dei dispositivi sono aumentate, facendoli diventare sempre più intelligenti e autonomi. L'aumento della loro complessità ha fatto sì che anche le reti divenissero sempre più sofisticate e performanti, intaccando l'intera infrastruttura IoT e rendendo il nostro grado di interazione con gli oggetti sempre più fluido, intuitivo e immersivo.

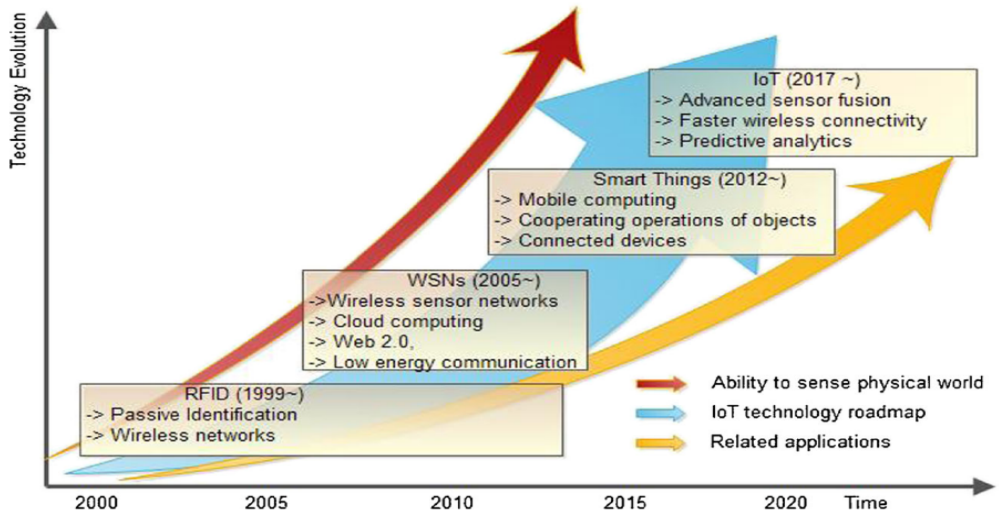

Figura 1.1: Evoluzione dell'IoT

Al giorno d'oggi, le Thing possono variare da semplici prodotti muniti di Auto-ID tag (codici a barre, codici QR, NFC e RFID tag) così da poter essere monitorati durante i loro spostamenti, fino a sistemi ad alta complessità come ad esempio un'automobile, un edifico o persino un'intera città. L'obiettivo dell'IoT è quello di rendere le Thing connesse ovunque e in qualsiasi momento, con chiunque e con qualunque cosa. Per questo motivo ad ogni Thing viene attribuito un identificatore univoco universale (UUID) che le permette di essere individuata e acceduta univocamente all'interno della rete.

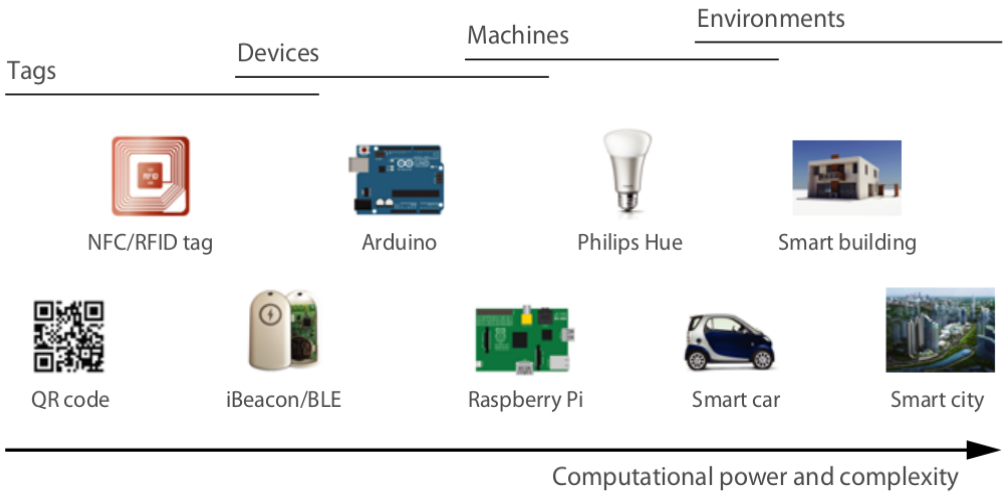

Figura 1.2: Tipologie di Thing

1.1 Architettura dell'IoT

Un requisito fondamentale del paradigma IoT è quello di rendere le Thing presenti in rete interconnesse tra loro, in grado di comunicare e scambiare informazioni. Il suo soddisfacimento, però, viene complicato dalla miriade di Thing presenti in commercio, ognuna con uno specifico hardware e uno specifico software che, il più delle volte, le rendono incompatibili e incapaci di comunicare. Oltre a questo, si aggiunge il fatto che Thing diverse possono essere utilizzate per uno

stesso scenario poiché, ad esempio, eseguono la stessa funzione. Quindi deve essere presente un sistema di regole che stabilisca in che modo le diverse tecnologie si relazionino le une con le altre e quale configurazione scegliere nel deployment dei differenti scenari. Questo sistema di regole prende il nome di architettura dell'IoT.

L'architettura dell'IoT è costiuita da quattro livelli, ognuno dei quali specifica una diversa funzionalità[2]:

1. **Livello di Sensing**
   Fanno parte di questo livello i sistemi hardware e i loro sensori. Questi ultimi sono in grado di collezionare dati provenienti dall'ambiente esterno, come ad esempio: temperatura, umidità, qualità dell'aria, velocità, rumore, pressione, movimento ecc. In alcuni casi possono avere una minima capacità di storage al fine di memorizzare un certo numero di misurazioni. Queste misurazioni, poi, sono convertite in segnali comprensibili alla Thing a esso collegata.
   Nel determinare il livello di sensing di un'applicazione IoT bisogna tener conto di diversi fattori, tra cui il costo, la dimensione, le risorse e il consumo di energia dei sensori, la politica di deployment, l'eterogeneità, la tipologia di comunicazione e di rete (es. ZigBee, Z-Wave, Bluetooth, WiFi, Ethernet ecc).
2. **Livello di Rete**
   In questo livello viene definita la configurazione della rete all'interno della quale sono connesse le Thing. In primo luogo, la tecnologia di rete deve essere tale da supportare la comunicazione machine-to-machine (M2M), altrimenti le Thing non potrebbero comunicare e scambiare dati tra loro. Si deve mantenere un Quality of Service (QoS) standard, in modo tale che le prestazioni della rete non crollino a causa dell'elevato numero di Thing connesse o dell'elevato traffico. Deve essere sempre possibile scoprire automaticamente e mappare le nuove Thing che si connettono alla rete. E infine, si deve garantire la sicurezza dei dati che viaggiano in rete, soprattutto perché essi possono contenere informazioni confidenziali, sia che si tratti di applicazioni per privati, sia di applicazioni aziendali. Questo ultimo punto è il più complesso da gestire per due motivi principali: il primo, è che l'aggiunta di un livello

di sicurezza aumenta la complessità dell'intera applicazione e il secondo, è che l'implementazione del protocollo di sicurezza al livello di Thing viene limitata fortemente dalla ridotta capacità computazionale che hanno alcune di esse. Per cui o si fornisce una sicurezza di base o la si sposta al livello applicativo.

3. **Livello di Servizio**
   Fanno parte di questo livello le tecnologie middleware. Esse offrono tutta una serie di servizi (es. API) che vengono eseguiti direttamente in rete e che si posizionano ad un livello superiore rispetto alle Thing. Infatti, questa tipologia di servizi sono dedicati alla raccolta, gestione e analisi dei dati prodotti dalle Thing (es. dati che provengono dalle attività di sensing), al fine di fornire strumenti di controllo ali utenti o alle applicazioni.
4. **Livello di Applicazione**
   Il livello di applicazione è l'ultimo livello dell'architettura dell'IoT, si trova al livello più elevato di astrazione ed è rappresentato dall'interfaccia dell'intero sistema IoT a cui l'utente può accedere, sulla quale sono esposti i metodi di interazione con il sistema sottostante (costituito da servizi, rete e sensori). L'interfaccia permette all'utente di accedere ai servizi forniti dalle differenti Thing presenti nel sistema IoT, cosa che non potrebbe fare in assenza, dato che, il più delle volte, esse appartengono a fornitori diversi e di conseguenza possono non rispettare gli stessi protocolli e standard. Quindi, in conclusione, l'interfaccia rende compatibili tra loro Thing eterogenee e fornisce meccanismi che facilitano la loro gestione e la loro interconnessione.

1.2 Interoperabilità nell'IoT

Il livello di applicazione dell'infrastruttura dell'IoT ci ha introdotto il concetto di compatibilità tra Thing. Soltanto Thing compatibili tra loro sono in grado di comunicare e scambiare informazioni. Ora la domanda che ci si pone è la seguente: come si fa a rendere Thing diverse compatibili tra loro? Ed è dalla ricerca della risposta a questa domanda che nasce il problema dell'interoperabilità.

L'associazione internazionale IEEE (Institute of Electrical and Electronics Engineers) ha definito l'interoperabilità come *"la capacità di due o più sistemi o componenti di scambiarsi informazioni e di saper interpretare e utilizzare le informazioni scambiate"*[4].

Esistono diversi livelli di interoperabilità[5], all'incirca uno per ogni livello dell'interfaccia dell'IoT. Ora di seguito li andremo ad esaminare.

- **Interoperabilità di dispositivo**
  L'interoperabilità al livello di dispositivo riguarda la capacità di rendere dispositivi eterogenei (con hardware, software, protocolli e standard di comunicazione differenti) capaci di scambiare informazioni e così di fare in modo che ogni genere di dispositivo possa essere integrato in una qualsiasi piattaforma IoT.
  Si distinguono due categorie principali di dispositivi: high-end e low-end. I dispositivi high-end (es. Raspberry Pi o smartphone) hanno sufficienti risorse e capacità computazionali da poter essere considerati a tutti gli effetti dei mini-calcolatori, mentre i dispositivi low-end (es. RFID-tag, sensori, attuatori, Arduino), al contrario, hanno ridotte capacità computazionali e risorse, in termini di durata della batteria, velocità del processore, RAM e protocolli di comunicazione e per entrambe le categorie, ogni caratteristica varia da dispositivo a dispositivo.
- **Interoperabilità di rete**
  Si sale di complessità, ora non si considerano più i dispositivi come entità isolate ma come entità interconnesse in rete. Nell'interoperabilità di rete non si fa riferimento ad un'unica rete ma a più reti (rete di reti), dove ad ognuna delle quali è connesso un dispositivo diverso. L'obiettivo è quello di far comunicare tra loro sistemi connessi a reti diverse (ad esempio tramite gateway) e fare in modo che lo scambio di messaggi sia il più possibile senza interruzioni. L'interoperabilità di rete, quindi, si dovrà occupare della gestione degli indirizzi di rete, del routing, del QoS, dell'ottimizzazione delle risorse, della sicurezza ecc.

- **Interoperabilità sintattica**

  L'interoperabilità sintattica definisce le regole da seguire circa il formato e la struttura dei dati scambiati tra sistemi eterogenei. Per fare in modo che i dati che viaggiano in rete siano interpretabili da due o più sistemi differenti, è necessario che essi concordino una grammatica comune per definire le regole sintattiche di codifica e decodifica dei messaggi scambiati. Nel caso in cui, invece, le regole di codifica del sistema mittente siano incompatibili con quelle di decodifica del sistema destinatario, si avrà un mismatch nel parse tree del processo di decodifica del messaggio, risultando, di fatto, incomprensibile al destinatario.

  Esempi concreti di schemi sintattici sono le API RESTful e WSDL o ad un livello più basso, i formati di serializzazione JSON e XML.

- **Interoperabilità semantica**

  Al livello successivo dell'interoperabilità sintattica, c'è l'interoperabilità semantica, essa viene definita dal World Wide Web Consortium (W3C) come l'attivazione di agenti, servizi e applicazioni con il fine di fare in modo che i dati e la conoscenza vengano scambiati in modo significativo (con un significato di senso compiuto), sia dentro che fuori dal Web. Il Web of Things affronta il problema tramite la condivisione di API da parte dei sistemi interconnessi. In questo modo essi sanno qual è il significato dei dati che ricevono e quali sono le operazioni da eseguire su di essi poiché, appunto, seguono lo schema definito dall'API in comune.

  L'interoperabilità semantica svolge anche un secondo compito: quello di rendere compatibili tra loro gli schemi del formato, definito dall'interoperabilità sintattica e del significato dei dati.

- **Interoperabilità di piattaforma**

  Al livello più alto si posiziona l'interoperabilità di piattaforma, che si occupa di rendere compliant piattaforme software differenti al fine di poter integrare i dati provenienti da ciascuna di esse.

  L'interoperabilità di piattaforma nasce per definire le linee guida per l'uso dei diversi sistemi operativi, linguaggi di programmazione, strutture dati, archi-

tetture e meccanismi di accesso propri delle Thing e dei dati da esse prodotti. Esistono diversi sistemi operativi specifici per dispositivi IoT, come ad esempio Contiki[1], RIOT[2], TinyOS[3] e OpenWSN[4], tutti con diverse versioni disponibili. Dall'altra parte, anche i fornitori di piattaforme IoT come Apple HomeKit[5], Android Things[6], Amazon AWS IoT[7] e IBM Watson[8] hanno i propri sistemi operativi, linguaggi di programmazione e strutture dati.
Per concludere, si può dire che è proprio grazie all'interoperabilità di piattaforma che è possibile sviluppare applicazioni multi-piattaforma a cui l'utente si può interfacciare e gestire i dati provenienti da ognuna di esse.

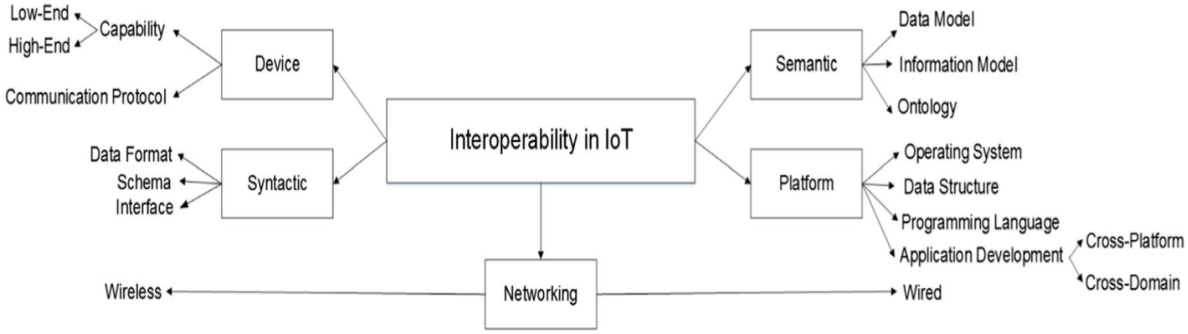

Figura 1.3: Tipologie di Interoperabilità

Senza interoperabilità, gli sviluppatori avranno l'obbligo di adattare le loro applicazioni alle specifiche delle piattaforme che andranno ad utilizzare, costringendoli in questo modo a rimanere confinati all'interno della stessa o delle stesse tipologie di piattaforme compatibili con i loro use case. Per di più, le funzionalità di queste piattaforme sono spesso limitate ai pochi utilizzi pensati e proposti dal loro produttore.

[1] https://www.contiki-ng.org/
[2] https://www.riot-os.org/
[3] http://www.tinyos.net/
[4] http://www.openwsn.org/
[5] https://www.apple.com/it/shop/accessories/all-accessories/homekit
[6] https://developer.android.com/things
[7] https://aws.amazon.com/iot/
[8] https://www.ibm.com/cloud/watson-iot-platform

L'importanza dell'interoperabilità nell'IoT è stata enfatizzata sia dall'accademia che dal settore industriale. La strada che si è scelto di percorrere è quella della standardizzazione, cioè la definizione di standard che rappresentino la base di riferimento da seguire per la realizzazione di tecnologie fra loro compatibili.

A questo punto si può procedere in due modi: il primo è quello di definire da zero nuovi standard ad-hoc, specifici per le tecnologie del mondo dell'IoT, mentre il secondo è quello di sfruttare standard già esistenti e adattarli a questo mondo. Il metodo scelto dal Web of Things è proprio quest'ultimo, con l'idea di utilizzare gli standard, i protocolli e i blueprint del Web.

Capitolo 2

W3C Web of Things

Il World Wide Web Consortium (W3C) è una comunità internazionale i cui membri, uno staff a tempo pieno e il pubblico, lavorano insieme per sviluppare gli standard web[7]. Nel 2015, il W3C ha istituito un Working Group per lavorare alla standardizzazione del WoT. Lo scopo del gruppo è stato, ed è tuttora, quello di contrastare la frammentazione dell'IoT attraverso una serie di componenti standard (meta-dati, API, ecc.) che consentono una facile integrazione tra piattaforme IoT e domini applicativi[8].

Il lavoro del W3C è stato reso necessario anche dal fatto che, nel corso degli anni, non si è riusciti a definire uno standard o un protocollo universale abbastanza forte da indirizzare i produttori e gli sviluppatori di sistemi IoT verso un'unica direzione, nonostante le continue proposte da parte di diversi organismi di standardizzazione, alleanze industriali e venditori in generale.

Il Web of Things parte da una Thing fisica e la virtualizza, cioè ne crea una copia esatta virtuale (*digital twin*) accessibile dall'utente tramite le tecnologie del web. L'utente accede direttamente alla copia virtuale senza che si debba preoccupare della posizione fisica della Thing stessa o di quali protocolli siano stati utilizzati per accedervi.

2.1 Architettura del WoT

Di seguito si andrà a descrivere l'architettura del WoT e le sue componenti. Nel farlo si farà riferimento alle ultime pubblicazioni (*draft*) del W3C pubblicate nel 2020[9], tenendo presente però che sono documenti in continua evoluzione (ed in parte incompleti) e possono subire dei cambiamenti importanti sia da un punto di vista strutturale che di contenuto.

A grandi linee, il fine dell'architettura del WoT è quello di descrivere ciò che esiste piuttosto di dire cosa deve essere implementato, non viene definito nessuna tecnologia o implementazione concerta. Per questo motivo si descrive un'architettura astratta, basata su un insieme di requisiti derivanti da vari casi d'uso (use-case), ognuno per un diverso dominio applicativo. Questi requisiti sono classificati in base all'ambito di applicazione in diverse "categorie" chiamate *building blocks*, che possono essere viste come i pilastri che ogni piattaforma che si basa sul Web of Things deve rispettare (processo di standardizzazione). L'architettura del WoT li descrive uno per uno e definisce il modo in cui sono correlati. I building blocks, poi, possono essere mappati su una varietà di deployment concreti.

Le varie sezioni dell'architettura possono essere normative o informative e per ognuna lo si andrà a specificare.

2.1.1 Casi d'uso

Questa sezione è informativa.

Di seguito si andranno ad elencare i casi d'uso presi in esame dal W3C come punti di partenza per derivare l'architettura astratta.

- Consumer (utente o consumatore finale)
  - applicazioni di Smart Home (es. domotica)
- Industriale
  - monitoraggio e previsione di possibili guasti e anomalie dei macchinari
  - applicazioni di Smart Factory

- Trasporti e logistica
  - monitoraggio di veicoli, di costi del carburante e di manutenzione degli stessi
  - tracciamento di spedizioni per garantire la loro condizione e qualità
- Utilità
  - lettura automatica di contatori residenziali, commerciali e industriali
  - monitoraggio delle condizioni e della produttività delle risorse rinnovabili
- Assicurazioni
  - monitoraggio dei rischi aziendali al fine di ridurre gli incidenti ed aumentare la sicurezza sul lavoro
  - monitoraggio delle previsioni del meteo al fine di re-instradare il traffico per evitare danni provocati dalla grandine o dalla caduta degli alberi
- Agricoltura
  - monitoraggio delle condizioni del terreno e definizione di piani ottimali per l'irrigazione e la concimazione
  - monitoraggio degli andamenti della produzione agricola
- Sanità
  - raccolta ed analisi di dati dagli studi clinici
  - controllo remoto di pazienti dopo il ricovero in ospedale
- Monitoraggio ambientale
  - monitoraggio dei livelli di inquinamento dell'aria, dell'acqua, della radioattività, ozono, temperatura, umidità ecc...
- Smart Cities
  - monitoraggio di ponti, dighe, canali per certificare le condizioni dei materiali e il loro deterioramento

  - costruzione di parcheggi intelligenti (*smart parking*) al fine di ottimizzare e monitorare la gestione degli spazi disponibili ed automatizzare i pagamenti e le prenotazioni
  - controllo intelligente dei semafori
  - monitoraggio ed ottimizzazione della gestione dei rifiuti
- Smart Buildings
  - monitoraggio del consumo energetico negli edifici
  - raccolta di feedback sulla soddisfazione degli inquilini riguardo all'abitabilità dei loro edifici
- Automobili
  - monitoraggio dello stato operativo ed ottimizzazione della manutenzione
  - miglioramento della sicurezza del conducente grazie ad un sistema di notifiche preventive sulle strade più pericolose e sulle condizioni del traffico

Oltre ai casi d'uso appena discussi, il W3C definisce anche dei pattern per illustrare come i dispositivi e le Thing interagiscono con i controller, con altri dispositivi, con agenti e server. Sono specificati sia pattern semplici come *Device Controllers* e *Thing-to-Thing*, sia pattern più complessi come *Digital Twins* e *Cross-domain Collaboration*. Questi ultimi due casi sono sicuramente i più interessanti: infatti il primo identifica una rappresentazione virtuale di uno o più dispositivi, mentre il secondo è una dimostrazione di come si possano connettere tra loro numerosi sistemi, che utilizzano protocolli o standard differenti, in un unico ecosistema.

2.1.2 Thing

Questa sezione è normativa.

Al centro dell'architettura del WoT c'è il concetto di Thing o Web Thing. Una Thing è un'astrazione di un'entità fisica (es. un dispositivo o una stanza) o virtuale (composizione di una o più Thing, es. una stanza con diversi sensori e attuatori, ognuno dei quali è a sua volta una Thing), descritta tramite un'insieme di meta-dati che seguono un determinato formato e vocabolario standard. Questo insieme di meta-dati prende il nome di *Thing Description* (TD) ed è basato sul formato JSON (JavaScript Object Notation).

La Thing Description rappresenta una vera e propria interfaccia che viene processata dai *Consumers* per poter accedere alla Thing stessa. Un Consumer può essere sia una persona fisica, sia un dispositivo elettronico, sia un'altra Thing. Nel momento in cui un Consumer andrà a visualizzare la Thing Description, esso potrà accedere a tutte le funzionalità che la Thing implementa.

Una Thing, per essere definita tale, da un lato DEVE avere almeno una TD e dall'altro, NON è possibile che più Thing condividano la stessa TD.

Il verbo utilizzato per indicare l'azione di visualizzazione della TD così da poter essere processata dai Consumers è *esporre*, mentre il verbo che indica l'azione effettuata dai Consumers di accedere alla TD e di eseguire le funzionalità della Thing è *consumare*. Perciò, è possibile consumare solo Thing che sono state esposte e una Thing esposta prende il nome di ExposedThing, mentre una Thing consumata prende il nome di ConsumedThing.

Figura 2.1: Interazione tra Consumer e Thing

Una Thing dovrà essere hostata in rete, in modo tale che potrà essere acceduta tramite un URI (Uniform Resource Identifier) ed internamente dovrà implementare uno stack software che, tramite l'interfaccia web, ne permetterà l'interazione.

Un tipico scenario in tal senso è rappresentato da un server HTTP in esecuzione su un dispositivo embedded (es. Arduino) con sensori e attuatori che implementa lo stack sotware ed espone la sua descrizione astratta sul web.

Può accadere che la rete locale dove è collegata la Thing non sia raggiungibile dalla rete Internet. Questo può accadere per colpa di dispositivi quali NAT (Network Address Translation) o firewall. Per rimediare a questa situazione il W3C WoT introduce l'entità di intermediario che si posiziona tra Thing e Consumer.

L'intermediario agisce come un proxy per la Thing ed ha una sua TD sulla quale è linkata la TD della Thing a cui fa riferimento. Dal lato del Consumer, il fatto che ci sia o meno un intermediario non cambia. La sua presenza è resa trasparente dal fatto che anche lui ha una TD, per cui risulta indistinguibile dal normale concetto di Thing.

Gli intermediari possono estendere le funzionalità di una Thing oppure possono creare una Thing virtuale componendo più Thing concrete.

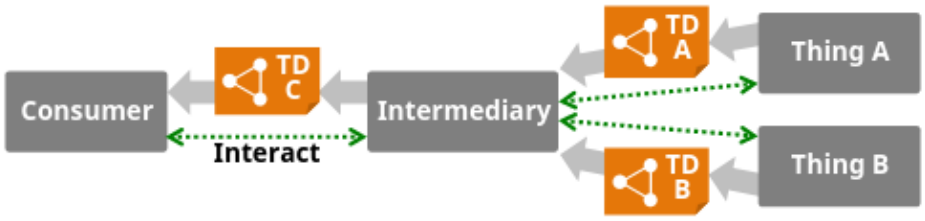

Figura 2.2: Intermediario

Successivamente si andranno ad analizzare i quattro Building Blocks, necessari al fine di implementare sistemi che risultino conformi all'architettura del WoT.

2.1.3 Thing Description

Questa sezione è informativa.

La WoT Thing Description[10] è un building block fondamentale e può essere considerata come l'entry point di una Thing (come lo è, ad esempio, la pagina *index.html* di un sito Web). La TD definisce due componenti: un modello di informazione basato su un vocabolario semantico che deve essere rispettato dalla Thing corrispondente e, come si è detto precedentemente, una rappresentazione serializzata basata sul formato dei dati JSON. Sia il modello di informazione che il formato di rappresentazione sono allineati con i Linked Data[11], in questo modo le varie implementazioni possono scegliere di utilizzare il formato JSON-LD[12] e i database a grafo per sfruttare al massimo l'elaborazione dei meta-dati.

E' stato scelto il formato JSON per due motivi principali: il primo è che è ampiamente diffuso nelle applicazioni Web, pe cui non va a incidere sulla curva di apprendimento dei sistemi WoT, il secondo è che è comprensibile dai dispositivi informatici, per cui è particolarmente adatto per applicazioni che implementano comunicazioni machine-to-machine (M2M). Per ora, il formato JSON-LD offre un buon compromesso tra semantica comprensibile alla macchina e usabilità per gli sviluppatori.

La TD ha cinque componenti principali: i meta-dati testuali, dei quali ne abbiamo già parlato in precedenza, che descrivono la Thing stessa (es. nome della Thing, ID, descrizioni ecc.), un insieme di *Interaction Affordances* che indicano le modalità con cui si può interagire con la Thing e quali sono le sue funzionalità, una serie di schemi sintattici sui dati per fare in modo che le Thing li comprenda, i *Web links*, utilizzati per esprimere qualsiasi relazione, sia formale che informale, ad altre Thing o ad altri documenti presenti sul web e infine le specifiche sulla sicurezza.

Per quanto riguarda le Interaction Affordances, il W3C ne definisce tre tipi: *Proprietà*, *Azioni* ed *Eventi*.

- **Proprietà**

  Una proprietà espone lo stato di una Thing (può essere vista come una variabile dei linguaggi di programmazione). Ad una proprietà, si deve sempre poter accedere in lettura, mentre l'accesso in scrittura è opzionale. E' inoltre possibile rendere una proprietà osservabile: in questo caso al Consumer verrà

notificato ogni cambiamento di stato della Thing con un messaggio push. Esempi di proprietà sono i valori misurati di un sensore (es, temperatura, umidità ecc.), lo stato di un attuatore o i parametri di configurazione.

- **Azione**
  Un'azione consente di invocare una funzione sulla Thing. La sua invocazione può produrre come effetto un cambiato di uno o più stati di una Thing. Esempi di azioni sono la regolazione della luminosità di una lampadina o la stampa di un documento.
- **Eventi**
  Un evento corrisponde ad una condizione, la quale, nel momento in cui si verifica, innesca un invio asincrono di messaggi push verso il Consumer. Non viene comunicato lo stato ma vengono comunicati i cambiamenti di stato di una Thing. Solitamente, per poter ricevere i messaggi in seguito al verificarsi di un evento, un Consumer deve prima sottoscriversi all'evento stesso. Di contro, un Consumer può anche decidere di cancellarsi da un evento per non riceverne più i messaggi.
  Un esempio di un evento è l'innesco di un allarme.

Di norma, per ogni Interaction Affordance si espone un endpoint (un URI), accedendo al quale si può visionare il valore di uno stato della Thing per le proprietà, invocare una funzione per le azioni e sottoscriversi ad un evento.

Le Thing, generalmente, salvano la propria TD in una directory che agisce da cache, velocizzandone così l'accesso e l'utilizzo da parte dei Consumers e facilitando la gestione dei sensori e attuatori connessi.

```
{
    "@context": "https://www.w3.org/2019/wot/td/v1",
    "id": "urn:dev:ops:32473-WoTLamp-1234",
    "title": "MyLampThing",
    "securityDefinitions": {
        "basic_sc": {"scheme": "basic", "in":"header"}
    },
    "security": ["basic_sc"],
    "properties": {
        "status" : {
            "type": "string",
            "forms": [{"href": "https://mylamp.example.com/status"}]
        }
    },
    "actions": {
        "toggle" : {
            "forms": [{"href": "https://mylamp.example.com/toggle"}]
        }
    },
    "events":{
        "overheating":{
            "data": {"type": "string"},
            "forms": [{
                "href": "https://mylamp.example.com/oh",
                "subprotocol": "longpoll"
            }]
        }
    }
}
```

Figura 2.3: Thing Description

2.1.4 Binding Templates

Questa sezione è informativa.

In una piattaforma IoT può essere presente qualsiasi tipologia di dispositivi, ognuno con un differente set di componenti e di protocolli di comunicazione. Questo perché non esiste un singolo protocollo che vada bene per qualsiasi scenario ed è per questo motivo che il Web of Things si sta focalizzando sullo studio di come rendere dispositivi diversi interoperabili.

L'obiettivo dei Binding Templates[13] è quello di fornire un insieme di meta-dati e blueprint di comunicazione che specificano il modo in cui si deve interagire con le differenti piattaforme IoT (es. OCF[9], oneM2M[10], Mozilla IoT[11], ecc.).

Per ogni tipologia di piattaforma IoT, i Binding Templates illustrano quali siano i protocolli a cui meglio si adatta e per ogni protocollo hanno associati i meta-data che devono essere aggiunti alla TD. Ovviamente, si fa riferimento soltanto a quei protocolli che supportano le tecnologie del Web come ad esempio HTTP, COAP o MQTT. Nella scelta del protocollo di comunicazione si deve tener conto del tipo di architettura sottostante e di quali metodi espone. Esempi di pattern architetturali sono Restful e PubSub, mentre esempi di metodi ad essi collegati sono GET, PUT, POST, DELETE, PUBLISH e SUBSCRIBE.

I Consumers che consumano una TD devono implementare il corrispondente Protocol Binding per poter accedere alle funzionalità della Thing e invocarne le funzioni, andando ad includere lo stack tecnologico necessario e la sua configurazione in base alle informazioni trovate nella TD stessa.

[9] `https://openconnectivity.org/`
[10] `http://www.onem2m.org/`
[11] `https://iot.mozilla.org/`

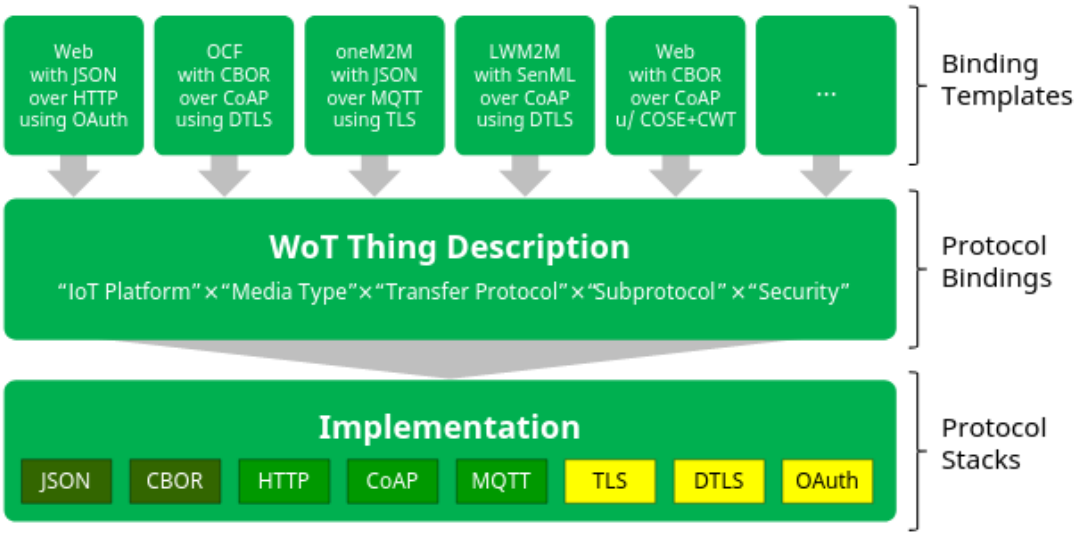

Figura 2.4: Dai Binding Templates ai Protocol Bindings

I meta-dati di comunicazione dei Protocol Bindings si estendono su cinque dimensioni:

- **IoT Platform**
  Le piattaforme IoT spesso introducono delle modifiche proprietarie ai protocolli, quali header HTTP specifici o opzioni CoAP. I Form presenti nella TD devono contenere le informazioni riguardo a queste modifiche.
- **Media Type**
  Le piattaforme IoT differiscono spesso nei formati di rappresentazione (o nella loro serializzazione) utilizzati per lo scambio dei dati. I Media Type servono proprio per identificare questi formati.
- **Transfer Protocol**
  Si tratta dei protocolli standard dello strato Applicazione (HTTP, MQTT, CoAP, ecc.) senza nessun tipo di opzioni specifiche o meccanismi di sotto-protocollo.
- **Subprotocol**
  I Transfer Protocol possono avere dei comportamenti particolari che richiedo-

no un'ulteriore specifica per poterci interagire con successo. Questa ulteriore specifica è il sotto-protocollo. Un esempio di sotto-protocollo è la tecnica *long polling* per HTTP che ovviamente non può essere identificata tramite lo schema standard dell'URI del Transfer Protocol.

- **Security**
  I meccanismi di sicurezza possono essere applicati a diversi livelli dello stack di comunicazione e possono essere anche utilizzati insieme, col fine di completarsi a vicenda.

2.1.5 Scripting API

Questa sezione è informativa.

Le Scripting API[14] sono un building block opzionale che definisce un insieme di API basate sulle specifiche di ECMAScript, simili alle API per Web browser. Le Scripting API vengono implementate in uno o più script eseguiti dalla Thing di riferimento e ne definiscono il suo comportamento, il comportamento dei Consumers e quello degli Intermediari.

Generalmente, la logica dei dispositivi IoT viene implementata a livello di firmware così da essere eseguita più velocemente e perfettamente compatibile con l'hardware del dispositivo. Nel caso delle Scripting API ciò non avviene, esse infatti, come si è detto nel paragrafo precedente, implementano la logica tramite script di programmazione che vengono eseguiti in un sistema runtime, chiamato WoT Runtime. L'utilizzo degli script dà un duplice vantaggio: da un lato, essi sono completamente riusabili, per cui possono essere utilizzati da altre applicazioni IoT senza dover essere riscritti da capo (a differenza del firmware che è specifico di ogni dispositivo), dall'altro, incrementano la produttività e riducono i costi di interoperabilità.

All'interno degli script vengono definite le strutture dati e gli algoritmi che permettono di produrre, esporre, consumare, fetchare e scoprire le Thing Descriptions. Il sistema runtime di una Thing istanzia una serie di oggetti che agiscono come interfacce per le altre Thing e per le loro Interaction Affordances.

Dato che le Scripting API necessitano di molte risorse per poter essere eseguite, solitamente vengono implementate sui nodi più potenti della rete, come per esempio i gateway.

Nelle Scripting API sono presenti tre elementi principali:

- **Oggetto API WoT**
  Questo oggetto rappresenta l'entry point dell'API, viene esposto come singleton e definisce i metodi per consumare, produrre e scoprire una Thing a partire dalla sua TD.
- **Interfaccia ConsumedThing**
  Rappresenta un'API client definita dal Consumer per operare sulla Thing: leggere, scrivere ed osservare proprietà, invocare azioni e sottoscriversi o cancellarsi ad un evento.
- **Interfaccia ExposedThing**
  Questa interfaccia estende l'interfaccia precedente e rappresenta l'API del server che esegue la logica della Thing. Al suo interno sono definiti gli handler per gestire le richieste (proprietà, azioni ed eventi) verso la Thing.

2.1.6 Security and Privacy Guidelines

Questa sezione è informativa.

La sicurezza è un problema trasversale nel WoT e dovrebbe essere considerata in ogni aspetto del design di un sistema, specialmente se nel sistema viaggiano dati sensibili. Le linee guida sulla sicurezza e sulla privacy si estendono a tutti i building blocks discussi precedentemente e per ognuno di essi si specificano quali sono i punti deboli, quali sono i principali attacchi che si possono subire e quali sono le contromisure da adottare.

Il documento sulla sicurezza e sulla privacy[15] ha uno scopo prettamente informativo, infatti non impone nessun modello concreto. Non introduce neanche nuovi meccanismi per la sicurezza, ma fa riferimento a quelli che sono già presenti sul mercato (crittografia a chiave privata, a chiave pubblica, OAuth ecc.). Fornisce anche una serie di test per validare il modello o i modelli di sicurezza scelti.

Le principali pratiche di sicurezza per i sistemi WoT sono le seguenti:

- **Pratiche di sicurezza nella progettazione di una Thing Description**
  - Proteggere i dati contenuti nella TD quando vengono acceduti, trasmessi in rete e salvati in uno spazio di archiviazione
  - Evitare l'esposizione di campi immutabili nella TD, specialmente se contengono informazioni associabili ad una particolare persona fisica
  - Minimizzare l'esposizione di informazioni pubbliche riguardanti una Thing (versione del software o sistema operativo)
  - Limitare gli accessi alla TD
- **Pratiche di sicurezza per la protezione dei dati sensibili nel sistema**
  - Utilizzare protocolli di comunicazione sicuri, come HTTPS (con TLS), CoAPS (con DTLS) e MQTTS (con TLS)
  - Informare gli utenti riguardanti quali informazioni personali possono essere esposte e quali no
- **Pratiche di sicurezza per la progettazione di interfacce di rete WoT**
  - utilizzare schemi di controllo degli accessi (autenticazione e autorizzazione)
  - Evitare l'esecuzione di processi funzionali complessi e pesanti computazionalmente senza autenticazione del Consumer
  - Minimizzare le funzionalità e la complessità delle interfacce di rete, mantenendo solamente quelle strettamente necessarie
  - Effettuare fasi di validazione e testing (inclusi i fuzz test) complesse e complete

Ogni sistema WoT si adatta meglio ad uno specifico meccanismo di sicurezza piuttosto che ad un altro. La sua scelta deve essere ponderata, tenendo presente che i modelli più sicuri sono anche i più complessi e i più dispendiosi al livello di risorse, per cui non possono essere implementati direttamente su quei dispositivi che hanno capacità computazionali ridotte (provocando un rallentamento o addirittura un

crash dell'intero sistema), ma soltanto sui nodi più potenti, come ad esempio i gateway.

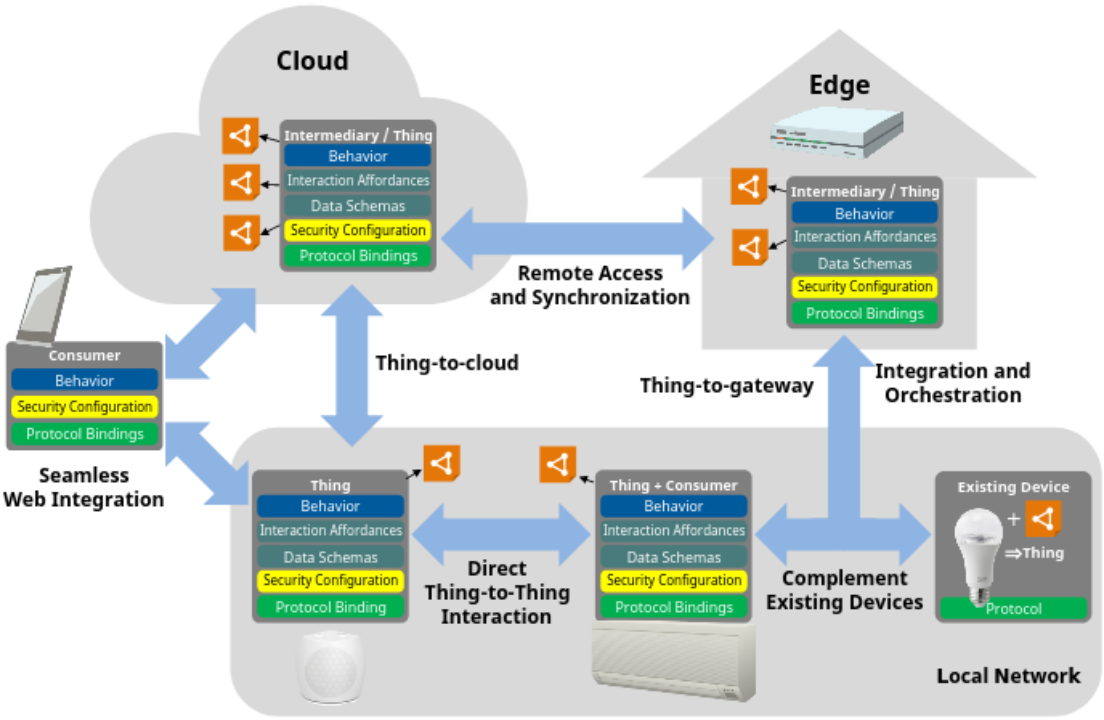

Figura 2.5: Architettura astratta del W3C WoT

Nella Figura 2.5 è mostrata una possibile configurazione di un'architettura del WoT, dove per ogni componente è specificata la struttura dei building blocks.

2.1.7 WoT Servient

Questa sezione è informativa.

Un Servient è uno stack software che implementa i building blocks visti precedentemente. Un Servient è in grado di eseguire, esporre e consumare le Thing e in base al Protocol Binding scelto, può agire sia come client che come server.

La comunicazione tra una ConsumedThing e un'ExposedThing implementate da due Servient può essere diretta o indiretta: è diretta nel caso in cui entrambi i

Servient utilizzano gli stessi protocolli di rete, risultando così mutualmente accessibili, mentre è indiretta nel caso contrario, cioè quando i Servient utilizzano protocolli diversi o sono connessi a reti differenti che necessitano di un'autorizzazione per potervi accedere (es. firewall).

Praticamente, un Servient è costituito dal codice di programmazione scritto dagli sviluppatori del sistema WoT che, prendendo in input la TD, le Scripting API e i Protocol Bindings, definisce la logica della Thing, le istruzioni che faranno parte del suo main loop, il modo in cui devono essere gestite le Interaction Affordances e il comportamento degli eventuali Consumers.

Se nelle sezioni precedenti abbiamo descritto l'architettura astratta del WoT, ora, attraverso il Servient, ne vedremo l'implementazione concreta.

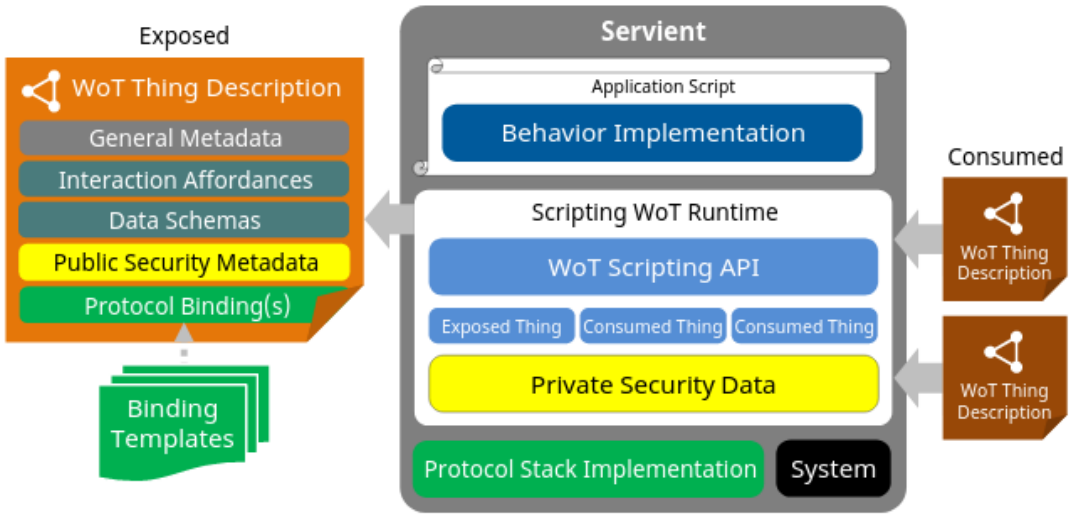

Figura 2.6: Implementazione di un Servient attraverso le Scripting API

Nella Figura 2.6 sono mostrati i moduli che compongono l'architettura di un Servient e anche se alcuni di loro li abbiamo già analizzati nelle sezioni precedenti, mancano ancora alcuni tasselli fondamentali per avere il quadro completo.

Di seguito verranno specificati, per ogni modulo, il suo ruolo e le sue funzionalità:

- **Behaviour Implementation**
  Il "comportamento" definisce la logica dell'applicazione eseguita dalla Thing. E' costituito da diversi aspetti: il comportamento autonomo della Thing (es. misurazioni dei sensori e loop di controllo per gli attuatori), gli handler per gestire le Interaction Affordances (ad es. il codice che viene eseguito concretamente quando un'interazione viene attivata), il comportamento del Consumer (che consuma la Thing) e il comportamento dell'Intermediario (es. fare da proxy per una Thing o comporre più entità virtuali).

- **WoT Runtime**
  La logica della Thing e il suo modello di interazione sono implementati in un sistema a runtime, chiamato WoT Runtime. Esso mantiene l'ambiente di esecuzione per l'implementazione del comportamento della Thing, è in grado sia di esporre e consumare Thing, sia di fetchare, processare, serializzare TD. Solitamente la logica dell'applicazione dovrebbe essere eseguita in un ambiente isolato in modo tale da prevenire accessi non autorizzati a dati sensibili (Private Security Data).
  Il WoT Runtime, poi, fornisce una serie di operazioni per gestire il ciclo di vita delle Thing (LCM) o, più precisamente, le loro astrazioni e descrizioni software, e per farlo utilizza un sistema di interfacce interne.
  Gli ulteriori compiti del WoT Runtime sono: l'implementazione dei Protocol Bindings definiti nei Binding Templates e l'interazione con il sistema sottostante della Thing per accedere all'hardware locale (sensori e attuatori) o agli spazi di archiviazione.
  Il WoT Runtime sfrutta le Scripting API per assolvere i suoi compiti.

- **Protocol Stack Implementation**
  Lo stack dei protocolli di un Servient, da un lato, implementa l'interfaccia delle ExposedThings, mentre dall'altro, viene utilizzato dai Consumer per accedere alle ConsumedThings (Thing remote). È il componente che produce i messaggi di protocollo concreti per interagire all'interno della rete.
  I Servient possono implementare più protocolli in modo tale da rendere la piattaforma IoT di riferimento interoperabile con le altre. In questo caso

però, per ogni protocollo supportato, deve essere presente la sua specifica nei Protocol Bindings.

- **System API**
  L?implementazione di un WoT Runtime può accedere all'hardware locale o ai servizi di sistema tramite API proprietarie o altri mezzi. Un dispositivo può trovarsi fisicamente esterno al Servient (dispositivo legacy), ma connesso tramite dei protocolli proprietari. In questo caso, il WoT Runtime può accedere al disposito legacy con questi protocolli e poi esporlo come Thing attraverso le Scripting API. Un Servient può agire come gateway per il dispositivo legacy, ma è un'opzione da considerare solo in caso non possa essere descritto tramite una TD. Questo meccanismo, però, non fa parte dello standard W3C WoT poiché ne limiterebbe la portabilità.

2.2 Implementazioni concrete del WoT Servient

Nella sezione precedente si sono descritti i componenti dell'architettura del Web of Things e l'implementazione astratta del WoT Servient.

In questa sezione, invece, si andranno ad esaminare due implementazioni concrete open-source del WoT Servient per Arduino, disponibili sui repository GitHub dei rispettivi sviluppatori, così da fare un confronto con l'implementazione oggetto di questo progetto.

Le implementazioni open-source del Web of Things non si fermano a due, ne sono state sviluppate molte altre, principalmente su piattaforme differenti dai sistemi embedded. Esse sono state raccolte nel corso degli anni dall'Interest Group del W3C[16], il quale gestisce un forum con il fine di discutere delle ultime novità tecniche, casi d'uso e requisiti del mercato open-source, riguardanti le tecnologie del Web e del Web of Things.

Per ogni implementazione viene fornito il link al sito web o al repository degli sviluppatori, il nome dell'organizzazione a capo del progetto, le piattaforme e i linguaggi di programmazione con cui è stata realizzata, la licenza e una breve descrizione[17].

2.2.1 WoT Arduino

WoT Arduino[18] è un'implementazione del WoT Servient per le schede Arduino UNO con Ethernet Shield (basato sul controller di rete Wiznet W5100) per la connessione in rete. È scritta in C++ ed è sviluppata dal W3C/ERCIM (European Research Consortium for Informatics and Mathematics).

Attraverso questo tool l'Arduino viene convertito in un Web Server configurabile, il quale può interagire con uno o più sensori o attuatori. Le richieste sono in gestite in un formato JSON non standard, in quanto si ha una diversa rappresentazione dei dati in memoria in modo da ridurre lo spazio da loro occupato. Infatti, gli sviluppatori hanno improntato tutto il progetto in tal senso, definendo dei meccanismi e delle strutture dati per diminuire sia la quantità di memoria occupata durante l'esecuzione del sistema che la complessità computazionale, in modo da velocizzare le interazioni tra client e server e tra server ed i suoi sensori o attuatori.

Gli oggetti in formato JSON sono rappresentati in memoria come nodi di alberi binari bilanciati (AVL). Essi vengono allocati staticamente tramite l'utilizzo di array poiché l'uso delle funzioni `malloc` e `free` potrebbe causare problemi ai microcontrollori.

Come per gli oggetti JSON, anche le Thing Properties sono rappresentate in memoria come nodi di alberi binari bilanciati ma, in questo caso, c'è da fare un passaggio in più. Dato che le proprietà sono implementate come array JSON associativi che mappano il nome della proprietà con il suo valore JSON (coppie nome-valore) mentre i nodi sono indicizzati con valori numerici, viene definita una tabella dei simboli (hash table) che mappa i nomi delle proprietà in simboli numerici.

Oltre alle Thing Proprerties, anche le Thing Actions e i Thing Events sono implementati tramite array JSON associativi con l'aggiunta di un handler che gestisce la loro invocazione.

E' presente, poi, un meccanismo di garbage collection basato sull'algoritmo di *mark and sweep* che viene invocato quando la memoria disponibile sta per terminare e le celle di memoria contenenti oggetti JSON non più raggiungibili

vengono reclamate.

Infine, per ridurre la dimensione dei messaggi scambiati in rete in formato JSON è presente un meccanismo di codifica e decodifica che li converte in binario e per ridurre lo spazio in memoria RAM occupato dalle variabili di tipo stringa, le si salva nella memoria flash tramite la macro `F`.

I protocolli utilizzati sono: HTTP al livello applicazione e TCP al livello trasporto.

Il tool si compone di 12 file di libreria, 11 file di implementazione e 1 sketch da flashare sull'Arduino.

Utilizzo

Innanzitutto occorre stabilire se usare per il Web Server un indirizzo IP fisso o dinamico tramite il protocollo DHCP. Allo stesso modo si può decidere di utilizzare un indirizzo IP e una porta prefissati per il gateway oppure il servizio di DNS multicast per individuarli dinamicamente.

Una volta stabilito questo, si può passare alla definizione della Thing e dei suoi componenti.

La Thing, in questa implementazione, viene gestita tramite un oggetto di tipo `Thing` che va dichiariato all'interno dello sketch principale. Sucessivamente si definiscono le proprietà della Thing e dato che sono gestite tramite una tabella dei simboli, implementata tramite la libreria *Names.h*, sono registrate come simboli. Un simbolo è un oggetto `Symbol` che viene definito a partire dal nome della proprietà in questione. Un esempio di dichiarazine di un simbolo è il seguente: `Symbol foo = names->symbol(F(''foo''));`.

Ad una proprietà si possono assegnare sia valori di tipo base, sia oggetti JSON. Nel caso di un valore di tipo base, lo si può assegnare direttamente all'oggetto `Thing` tramite il metodo `set_property(PROPERTY_NAME, JSON::TYPE(VALUE))`, nel caso invece di un oggetto, prima lo si deve dichiarare, poi si devono definire i suoi campi e solo successivamente lo si può assegnare alla Thing.
Per recuperare il valore di una proprietà si usa il metodo
`get_property(SYMBOL_TABLE_NAME, PROPERTY_NAME)`.

Anche le azioni e gli eventi devono essere registrati come simboli prima di poter essere invocati. Le azioni vengono invocate tramite il metodo
`int invoke(Symbol action, ResponseFunc response, ...)`. Se l'azione non prevede una risposta, allora si deve passare `NULL` come secondo parametro. I parametri successivi sono opzionali e rappresentano i parametri richiesti in input dall'azione. Se l'azione termina con successo, il metodo `invoke` ritornerà un id positivo che verrà inviato all'handler della risposta che è definito nel modo seguente:
`void (*ResponseFunc)(unsigned int id, Thing *thing, ...)`.
Per lanciare gli eventi, invece, si deve chiamare il metodo
`void raise_event(Symbol event, ...)`, il quale reindirizza la chiamata all'handler definito come segue: `void (*EventFunc)(Symbol event, Thing *thing, ...)`.

Per visualizzare la TD si utilizza il comando `print()`, mentre per invocare il garbage collector si usa il comando `WebThings::collect_garbage()` fornito dalla libreria *WebThings*. Questa libreria fornisce anche i metodi di gestione delle Interaction Affordances citati precedentemente.

All'interno del metodo `setup()` di Arduino si deve, obbligatoriamente, connettere il server alla rete e avviare il protocollo di trasporto tramite `transport.start()` ed esporre la TD. Nel metodo `loop()`, invece, si gestiscono la coda degli eventi con `event_queue.dispatch()` e le richieste verso la Thing attraverso il comando `transport.serve()`.

2.2.2 Arduino RDF Server

Arduino RDF Server[19] è, come WoT Arduino, un'implementazione compatibile con le schede Arduino UNO con Ethernet shield, scritta in C++ e sviluppata dal LIRIS Lab di Lione, in Francia.

Anche in questo caso l'Arduino viene convertito in un Web Server configurabile, il quale espone le funzionalità dei vari sensori e attuatori ad esso collegati, risponde alle richieste in formato RDF, gestisce le richieste di riconfigurazione e può essere riavviato senza la perdita dei dati di configurazione. Questo è possibile grazie al fatto che i dati vengono memorizzati nella memoria EEPROM.

Ogni funzionalità viene esposta tramite un *Servizio*, il quale è descritto tramite le RESTful Web API Hydra[12]. Un servizio può essere configurato, abilitato e disabilitato a runtime senza la necessità di flashare un nuovo sketch contenente le nuove istruzioni. Nel momento in cui si fa richiesta di un servizio viene invocata una funzione che interagisce con il sensore o con l'attuatore collegato e ne modifica lo stato. Le funzioni possono prendere in input o restituire in output delle variabili che prendono il nome di *Risorse*.

I pacchetti scambiati tra client e server vengono trasmessi tramite il protocollo CoAP al livello applicazione, mentre al livello trasporto si utilizza il protocollo UDP.

Il tool è composto da sette file: sei dei quali, *Coap.h*, *ResourceManager.h*, *Semantic.h*, *Coap.cpp*, *ResourceManager.cpp* e *Semantic.cpp*, sono librerie e loro implementazioni, mentre il restante, *WebServer_Hackfest.ino*, costituisce lo sketch da flashare sull'Arduino.

Utilizzo

Come prima cosa è necessario configurare quali funzioni devono gestire quali pin della scheda Arduino, in modo tale da avere una corrispondenza logica tra il servizio e il sensore o attuatore a cui fa riferimento.

In secondo luogo occorre definire la Thing Description ed i relativi servizi. Entrambi devono essere definiti all'interno della libreria *Semantic.h* in formato JSON. I servizi (scritti in Hydra) vanno definiti all'interno dell'array
`const char CAPABILITIES[] PROGMEM` e per ognuno bisogna specificare i seguenti campi:

- `@id`: URL del servizio
- `@type`: tipo di operazione in Hydra (tipo di default hydra:Operation)
- `method`: metodo di accesso al servizio (GET, POST o PUT)
- `label`: etichetta riferita al servizio (opzionale)

[12] `http://www.hydra-cg.com/`

- `expects`: identificatore della risorsa da passare in input alla funzione invocata dal servizio (solo per POST e PUT)
- `returns`: identificatore della risorsa restituita in ouptut (solo per GET e POST)

Prima di poter invocare un servizio è necessario abilitarlo tramite la richiesta PUT `enable`, alla quale si deve passare l'identificatore del servizio e il numero di pin dell'Arduino nei quali è collegato il sensore o l'attuatore oggetto del servizio. La richiesta PUT `reset`, invece, resetta tutti i servizi.

Una volta descritti i servizi si passa alla definizione delle relative funzioni. Esse vanno definite nel file *Semantic.cpp*, mentre nel file di libreria *Semantic.h* vanno inserite soltanto le intestazioni.

Una funzione non deve ritornare nulla (`void`) e deve avere obbligatoriamente i seguenti parametri:

- `uint8_t pin_count`: numero di pin utilizzati
- `uint8_t pins[n]`: array all'interno del quale vanno inseriti i numeri dei pin impiegati (`n` deve corrispondere a `pin_count`)
- `JsonObject& root`: documento JSON corrispondente al corpo della richiesta al servizio
- `uint8_t results`: array in cui sono memorizzati quei dati che verranno inviati al client come risposta dell'invocazione del servizio

Terminata la scrittura della funzione, la si deve linkare al corrispondente servizio nel file *WebServer_Hackfest.ino* tramite l'istruzione `coap.addOperationFunction(&FUNCTION_NAME, (char* )‘‘SERVICE_ID‘‘);` da inserire all'inizio della funzione `setup()` di Arduino. Infine si definiscono le risorse all'interno della libreria *Semantic.h*.

Come per i servizi, anche le risorse vanno definite in un array in formato JSON (`const char VARIABLE_NAME[] PROGMEM`), con la differenza che si ha bisogno di un array per ognuna di loro. L'array deve avere lo stesso nome della risorsa e deve contenere, tra gli altri, i seguenti campi obbligatori:

- `@type`: identificatore della risorsa che deve corrispondere a quello inserito nei campi `expects` e `returns` presenti nella definizione del servizio che la gestisce
- `value`: valore della risorsa (inizialmente è vuoto)

Infine, sempre in *Semantic.h*, si devono inserire all'interno dell'array `PGM_P const json_resources[] PROGMEM` i nomi degli array di ciascuna risorsa definiti precedentemente e contestualmente, si aggiorna la costante `RESOURCE_COUNT` per farla corrispondere al loro numero.

La TD con i relativi servizi è esposta nella root (`/`) del Web Server e può essere acceduta tramite una richiesta GET.

Se volessimo fare un parallelismo tra i componenti di Arduino RDF Server e quelli dell'architettura del WoT, potremmo dire che i servizi del primo corrispondono alle Interaction Affordances del secondo. In particolare, le proprietà e le azioni del WoT sono denominate risorse e funzioni in Arduino RDF Server. Per quanto concerne gli eventi in Arduino RDF Server, essi non sono ancora stati implementati. Il protocollo di comunicazione (Protocol Binding) scelto è CoAP, mentre le Scripting API sono le API Hydra.

In conclusione, le due implementazioni risultano essere incomplete, poiché offrono soltanto funzionalità di base e non supportano l'intero set di specifiche del Web of Things. Attualmente, esse non vengono aggiornate già da alcuni anni. La prima dal 2016, mentre la seconda dal 2017.

Parte 2

Embedded WoT Servient

Capitolo 3

Progettazione

3.1 Obiettivo

Conclusioni

Queste sono le conclusioni.

In queste conclusioni voglio fare un riferimento alla bibliografia: questo è il mio riferimento [3, 4].

Appendice A

Prima Appendice

In questa Appendice non si è utilizzato il comando: `\clearpage{\pagestyle{empty}\cleardoublepage}`, ed infatti l'ultima pagina 8 ha l'intestazione con il numero di pagina in alto.

Appendice B

Seconda Appendice

Bibliografia

[1] Primo oggetto bibliografia.

[2] Secondo oggetto bibliografia.

[3] Terzo oggetto bibliografia.

[4] Radatz J., Geraci A., Katki F. *IEEE standard glossary of software engineering terminology*. In: IEEE Std 610.12-1990 (1990).

[5] Noura M., Atiquzzaman M., Gaedke M. *Interoperability in Internet of Things: Taxonomies and Open Challenges*. In: Mobile Networks and Applications 24, 796−809 (2019).

[6] Manyika J., Chui M., Bisson P., Woetzel J., Dobbs R., Bughin J., Aharon D. *The internet of things: mapping the value beyond the hype*. In: McKinsey global institute. McKinsey Glob Inst 3 (2015).

[7] W3C. *About W3C* (2020). [ultima vista 24.02.2020]. URL: `https://www.w3.org/Consortium/`.

[8] W3C. *Web of Things Working Group* (2020). [ultima visita 24.02.2020]. URL: `https://www.w3.org/WoT/WG/`.

[9] W3C. *Web of Things (WoT) Architecture* (2020). [ultima visita 26.02.2020]. URL: `https://www.w3.org/TR/wot-architecture/`.

[10] W3C. *Web of Things (WoT) Thing Description* (2020). [ultima visita 26.02.2020]. URL: `https://www.w3.org/TR/wot-thing-description/`.

[11] Tim Berners-Lee. *Linked Data Design Issues* (2006). [ultima visita 26.02.2020]. URL: `https://www.w3.org/DesignIssues/LinkedData.html`.

[12] W3C. *JSON-LD 1.1* (2019). [ultima visita 26.02.2020]. URL: `https://www.w3.org/TR/2019/CR-json-ld11-20191212/`.

[13] W3C. *Web of Things (WoT) Binding Templates* (2020). [ultima visita 26.02.2020]. URL: `https://www.w3.org/TR/wot-binding-templates/`.

[14] W3C. *Web of Things (WoT) Scripting API* (2019). [ultima visita 26.02.2020]. URL: `https://www.w3.org/TR/wot-scripting-api/`

[15] W3C. *Web of Things (WoT) Security and Privacy Guidelines* (2019). [ultima visita 26.02.2020]. URL: `https://www.w3.org/TR/wot-security/`.

[16] W3C. *Web of Things Interest Group* (2020). [ultima visita 27.02.2020]. URL: `https://www.w3.org/WoT/IG/`.

[17] W3C. *Web of Things Implementations* (2020). [ultima visita 27.02.2020]. URL: `https://www.w3.org/WoT/IG/wiki/Implementations`.

[18] GitHub. *Web of Things Framework for Arduino* (2016). [ultima visita 27.02.2020]. URL: `https://github.com/w3c/wot-arduino`.

[19] GitHub. *Arduino RDF Server* (2017). [ultima visita 27.02.2020]. URL: `https://github.com/ucbl/arduinoRdfServer`.

Ringraziamenti

Qui possiamo ringraziare il mondo intero!!!!!!!!!!
Ovviamente solo se uno vuole, non è obbligatorio.