Relazione del progetto di Informatica III



Laurea Magistrale in Ingegneria Informatica

I Anno

A.A. 2021/2022

Modulo di Progettazione e

Algoritmi

Prof. Patrizia Scandurra

cod. 38068

Wasim Essbai

Matteo Locatelli

Nicola Zambelli 1053015

Sommario

[Introduzione 4](#_Toc96450123)

[Obiettivo 5](#_Toc96450124)

[W3C 6](#_Toc96450125)

[LoRaWan 7](#_Toc96450126)

[MAPE-K loop 9](#_Toc96450127)

[MQTT 10](#_Toc96450128)

[Chirpstack 11](#_Toc96450129)

[Iterazione 0 12](#_Toc96450130)

[Analisi dei requisiti 13](#_Toc96450131)

[R0 – Azioni di riconfigurazione per allungamento del ciclo di vita delle sentinelle: 13](#_Toc96450132)

[R1 – Azioni di auto-diagnosi manutentiva di risoluzione autonoma dei guasti: 13](#_Toc96450133)

[User-Stories 15](#_Toc96450134)

[Lato edge device: 15](#_Toc96450135)

[Lato application server: 16](#_Toc96450136)

[Lato watchdoge: 17](#_Toc96450137)

[Use Case Diagram 18](#_Toc96450138)

[Deployment Diagram 19](#_Toc96450139)

[Deployment Diagram Informale 19](#_Toc96450140)

[Deployment Diagram UML 20](#_Toc96450141)

[Iterazione 1 21](#_Toc96450142)

[Iterazione 2 22](#_Toc96450143)

[Iterazione 3 23](#_Toc96450144)

[Iterazione 4 24](#_Toc96450145)

[Iterazione 5 25](#_Toc96450146)

# Introduzione

## Obiettivo

Il progetto ha come finalità la creazione di una piattaforma edge-cloud con la funzione di monitoraggio ambientale. Parte integrante del progetto sono i dispositivi IoT (internet of Things), capaci di raccogliere dati con uno scarso consumo di risorse.

I vantaggi dell’utilizzo di una rete di dispositivi IoT per la raccolta di dati ambientali sono molteplici, come la vasta scalabilità della rete e il basso costo delle spese di manutenzione, rispetto ad una classica stazione di monitoraggio ambientale.

I protagonisti della rete di acquisizione sono i watchdog, gli edge-node ed infine il cloud server:

* I **watchdog** sono i nodi sentinella, hanno il compito di campionare i dati e trasmetterli ai nodi edge. Tali dispositivi sono mobili e alimentati a batteria, perciò l’obbiettivo è quello di massimizzare il loro ciclo di vita, minimizzando il consumo di risorse. Un protocollo di comunicazione wireless a basso profilo è il *LoRaWan* che sarà discusso in seguito. Tale tecnologia ci permette di connettere i watchdog ai nodi edge con un modesto impiego di energia.
* Gli **edge-node** hanno un ruolo centrale nel progetto, il loro compito è quello di fare da *bridge* tra i watchdog ed il cloud server. Essi si interfacciano con i watchdog attraverso il protocollo LoRaWan e con il cloud server per mezzo del protocollo MQTT, anch’esso uno standard ISO per la messaggistica leggera, che si appoggia al livello TCP/IP dell’internet.
* Il **cloud server** ha la funzione di acquisire e immagazzinare le informazioni che arrivano dagli edge-node, inoltre sarà capace di analizzare e interpretare i dati, pianificando delle operazioni *self-adaptive* in modo migliorare la qualità di *dependability,* al fine di minimizzare ed ottimizzare l’intervento umano sui dispostivi fisici. Questo tipo di approccio permette di ottenere una maggiore qualità delle acquisizioni dei dati e di risparmiare sui costi di manutenzione e riparazione.

## W3C

Il World Wide Web Consortium, anche conosciuto come W3C, è un'organizzazione non governativa internazionale che ha come scopo quello di favorire lo sviluppo di tutte le potenzialità del World Wide Web e diffondere la cultura dell'accessibilità della Rete. Al fine di riuscire nel proprio intento, la principale attività svolta dal W3C consiste nello stabilire standard tecnici per il World Wide Web inerenti sia i linguaggi di markup che i protocolli di comunicazione.

Nel nostro caso siamo interessati al paragrafo 4.1.10 della guida, sul monitoraggio ambientale:

*“Il monitoraggio dell'ambiente si basa in genere su molti sensori distribuiti che inviano i propri dati di misurazione a gateway comuni, dispositivi perimetrali e servizi cloud.*

*Il monitoraggio dell'inquinamento atmosferico, dell'inquinamento idrico e di altri fattori di rischio ambientale come polveri sottili, ozono, composti organici volatili, radioattività, temperatura, umidità per rilevare condizioni ambientali critiche può prevenire danni irreparabili alla salute o all'ambiente.”*

Un altro paragrafo di nostro interesse è il 4.2.6, quello sui Digital Twins, utile per simulare le componenti.

*“Un gemello digitale è una rappresentazione virtuale, ovvero un modello di un dispositivo o un gruppo di dispositivi che risiede su un server cloud o su un dispositivo edge. Può essere utilizzato per rappresentare dispositivi del mondo reale che potrebbero non essere continuamente online o per eseguire simulazioni di nuove applicazioni e servizi, prima che vengano distribuiti ai dispositivi reali.”*



## LoRaWan

La specifica LoRaWan è un protocollo di rete LPWA (Low Power, Wide Area) progettato per connettere in modalità wireless *"things"* alimentati a batteria in reti regionali, nazionali o globali e si rivolge ai requisiti chiave dell'Internet of Things, come bi-servizi di comunicazione direzionale, sicurezza end-to-end, mobilità e localizzazione.

*Perché proprio LoRaWan?*

LoRaWan offre una durata della batteria pluriennale ed è progettato per sensori e applicazioni che richiedono di inviare piccole quantità di dati su lunghe distanze. Di seguito si può osservare un confronto tra LoRaWan e le comunicazioni wireless maggiormente adottate, come le reti LAN(local Area Network) e le reti *Cellular*



WiFi e BTLE sono standard ampiamente adottati ma servono alle applicazioni che comunicano con dispositivi personali su piccole distanze. La tecnologia cellulare è perfetta per applicazioni che richiedono un elevato throughput di dati, ma devono disporre di una notevole fonte di alimentazione.

LoRaWan definisce il protocollo di comunicazione e l'architettura di sistema (livello applicativo del modello ISO/OSI) ,mentre LoRa è lo strato fisico della telecomunicazione (livello1 del modello OSI), che consente il collegamento a lungo raggio.

Immagine che contiene tavolo

Descrizione generata automaticamente

*LoRaWan per l'Europa*

LoRaWan definisce dieci canali, otto dei quali sono multi-data da 250 bps a 5,5 kbps, un singolo canale LoRa ad alta velocità di trasmissione dati, a 11 kbps e un singolo canale FSK a 50 kbps. La potenza di uscita massima consentita da ETSI (European Telecommunications Standards Institute) in Europa è +14dBM. Ci sono restrizioni sul ciclo di lavoro ma senza limiti di tempo massimo di trasmissione o di permanenza del canale.

## MAPE-K loop

*MAPE-K control loop* è stato introdotto da IBM nel loro *white paper*: *“An architectural blueprint for autonomic computing”.* L’intento è quello di creare un ambiente informatico con le capacità di autogestione e auto-adattamento dinamico a seconda delle *business policies* implementate. Il ciclo e suddiviso in 4 aree principali:

* Monitor: raccoglie i dati delle risorse gestite
* Analyze: Esegue complesse analisi dei dati e valuta i segnali dalla funzione monitor.
* Plan: Struttura le azioni necessarie per raggiungere gli obiettivi richiesti,

essa crea o seleziona una procedura da attuare per la configurazione desiderata nella risorsa gestita.

* Execute: modifica il comportamento della risorsa gestita utilizzando gli effettori, sulla base delle azioni consigliate dalla funzione di piano.



Il nostro obbiettivo è quello di utilizzare questo modello concettuale allo scopo di creare un MAPE-Kper ogni *adaptation-goals,* inoltre provvederemo a valutare quale attore della rete prende in carico una particolare funzione del MAPE-K.

## MQTT

TODO

## Chirpstack

TODO

# Iterazione 0

## Analisi dei requisiti

Di seguito vengono elencati gli obiettivi che si vogliono raggiungere con questo progetto.

### R0 – Azioni di riconfigurazione per allungamento del ciclo di vita delle sentinelle:

Dal momento che i dispositivi IoT(le sentinelle) sono portatili, quindi alimentati da batteria, si vuole ottimizzare la durata della batteria intraprendendo delle azioni correttive sulla loro configurazione. Delle possibili azioni potrebbero intervenire sulla gestione della potenza e della frequenza di trasmissione.

|  |  |  |  |
| --- | --- | --- | --- |
| Scenario | Goal | Fenomeno | Azione |
| S1 | Massimizzare la durata della batteria dei watchdog. | La batteria dei watchdog scende al di sotto di determinate soglie. (50%, 30%, 15%, 10%) | Al superamento di ogni soglia è necessario:   * Diminuire la frequenza di trasmissione dei dati da parte dei watchdog. * Diminuire la potenza di trasmissione dei watchdog. |

### R1 – Azioni di auto-diagnosi manutentiva di risoluzione autonoma dei guasti:

Si vuole rendere possibile la rilevazione automatica di guasti sulle sentinelle, identificando la sentinella danneggiata con le sue caratteristiche tecniche e geografiche. A seguito di un guasto si possono intraprendere due diverse tipologie di azioni:

* Correzione: insieme di azioni, che il sistema compie autonomamente, volte a ripristinare il corretto funzionamento del dispositivo.
* Allerta: se le azioni correttive non sono efficaci, viene mandato un messaggio di allarme per richiedere un intervento manuale.

Oltre a rendere robusta la rete di sentinelle, si vuole tutelare il sistema da possibili malfunzionamenti dovuti a guasti dei nodi edge. Questo può essere fatto introducendo diversi nodi edge che comunicano tra loro e cooperano, in modo che, a fronte di un guasto su uno di essi, intervenga un altro nodo edge funzionante per prendere in carico i compiti di quello guasto.

|  |  |  |  |
| --- | --- | --- | --- |
| Scenario | Goal | Fenomeno | Azione |
| S3 | Rendere il sistema in grado di gestire i guasti sui watchdog in maniera autonoma.  (*self-recovery)* | Watchdog silente, cioè non trasmette dati per un certo intervallo di tempo.  (Ad es. 60s) | Il nodo edge tenta ripristinare il corretto funzionamento del watchdog guasto tramite il suo riavvio. |
| S4 | Allerta in caso di guasto ad un nodo watchdog e identificazione esatta delle sue caratteristiche fisiche e geografiche. | Guasto ad un watchdog non recuperabile. | Il nodo edge allerta un operatore per un intervento manuale sul nodo watchdog .guasto indicando le sue caratteristiche. |
| S5 | Rendere il sistema in grado di gestire guasti ai nodi edge in maniera autonoma.  (*self-recovery*) | Guasto di un nodo edge: non riceve i dati inviati dai watchdog e, quindi, non può inoltrarli al server. | * L*’application server* ridistribuisce il traffico di dati che arrivava al nodo edge guasto verso altri nodi edge. * L*’application server* notifica il personale del guasto avvenuto. |
| S6 | Limitare la perdita di informazioni dovute a gusti all’*application server.* | Malfunzionamenti dell’*application server* che quindi non è in grado di ricevere e/o elaborare i dati trasmessi dai gateway. | * I nodi edge devono mantenere i dati ricevuti dai watchdog in un buffer locale finchè il server non riprende la sua operatività. * I nodi edge devono notificare il guasto ad un indirizzo di rete dedicato e ritenuto affidabile. |

L’avvenimento di guasti viene fatto secondo la tattica ping-echo. In particolare, le condizioni di verificabilità dei vari scenari sono:

* S3: ping mandato da un nodo edge, echo non mandato dal watchdog
* S5: ping mandato dal server e/o da un nodo edge, echo non mandato dal nodo edge destinatario
* S6: ping mandato dai nodi edge, echo non mandato dal server

Ping-Echo

TODO

## User-Stories

Le user stories sono suddivise in tre raggruppamenti, uno per attore della rete, questa soluzione ci permette di indentificare i diversi *use-case* che saranno essenziali nello *use case diagram UML.*

### Lato edge device:

-Requisito R0:

* Come nodo edge, voglio essere in grado di conoscere il livello della batteria delle sentinelle in modo da sapere quando il livello di batteria scende sotto determinate soglie (M)
* Come nodo edge, voglio poter diminuire la frequenza di trasmissione delle sentinelle in modo da allungare la durata della loro batteria. (E)
* Come nodo edge, voglio poter diminuire la potenza del segnale di trasmissione delle sentinelle in modo da allungare la durata della loro batteria. (E)

-Requisito R1:

* Come nodo edge, voglio essere in grado di sapere quando una sentinella è silente in modo da poter rilevare sui guasti. (M)
* Come nodo edge, voglio essere in grado di riavviare una sentinella guasta in modo da ripristinare il suo funzionamento. (E)
* Come nodo edge, voglio essere in grado di mandare messaggi a del personale in modo da avvisare che una sentinella è guasta e comunicare i suoi dati. (E)
* Come nodo edge, voglio poter mandare un messaggio di ping ad altri nodi edge in modo da verificare che siano in funzione. (M)
* Come nodo edge, voglio poter subentrare al posto di un altro nodo edge in modo da svolgere i suoi compiti. (E)
* Come nodo edge, voglio poter mandare dei messaggi di ping all’application server in modo da avere informazioni sul suo funzionamento. (M)
* Come nodo edge, voglio poter analizzare le risposte ai messaggi di ping mandati all’application server in modo rilevare se sta mal funzionando. (A)
* Come nodo edge, voglio poter mantenere i dati che ricevo in un buffer locale in modo da evitare perdite di dati quando l’application server non li può ricevere.(E)
* Come nodo edge, voglio essere in grado di mandare messaggi ad un indirizzo di rete assegnato in modo da avvisare che l’application server è malfunzionante.(E)

### Lato application server:

Requisito R0:

* Come application server voglio essere in grado di valutare lo stato di carica delle sentinelle in modo da sapere quando la loro autonomia oltrepassa una certa soglia. (A)
* Come application server voglio essere in grado di determinare la frequenza e potenza del segnale di trasmissione per le sentinelle in modo da allungare il loro ciclo di vita. (P)
* Come application server voglio essere in grado di analizzare il livello di traffico in ingresso ad un nodo edge in modo da rilevare situazioni di congestione del nodo. (A)
* Come application server voglio essere in grado di determinare la frequenza di trasmissione delle sentinelle in modo da diminuire il flusso di dati in arrivo ad un nodo edge congestionato. (P)
* Come application server voglio essere in grado di analizzare il livello di traffico di un nodo edge in modo da rilevare situazioni di sottoutilizzo della rete. (A)
* Come application server voglio essere in grado di determinare la frequenza di trasmissione delle sentinelle in modo da aumentare il flusso di dati in arrivo ad un nodo edge. (P)

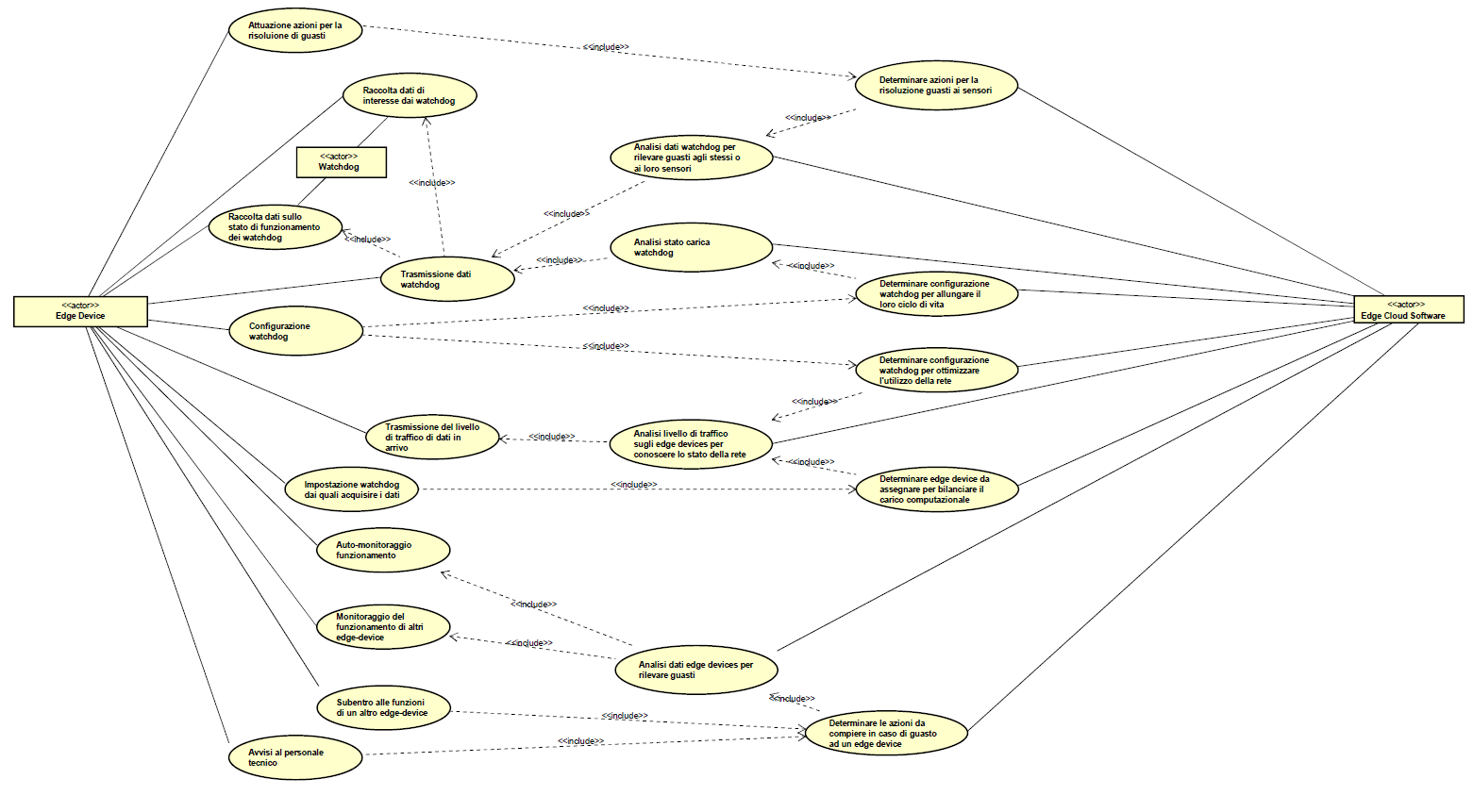
Requisito R1:

* Come application server, voglio poter fare delle analisi sui dati(le risposte ai ping) delle sentinelle ricevuti dal nodo edge in modo da sapere quando una sentinella è guasta. (A)
* Come application server, voglio poter fare delle analisi sui dati(le risposte ai ping) delle sentinelle ricevuti dal nodo edge in modo da sapere quando un sensore di una sentinella è guasto (A)
* Come application server, voglio poter comunicare ad un nodo edge di riavviare una sentinella in modo da ripristinare il suo funzionamento. (P)
* Come application server, voglio poter decidere quale nodo edge assegnare ad un gruppo di sentinelle in modo da subentrare ai compiti di un nodo edge malfunzionante o guasto. (P)
* Come application server, voglio poter inviare un messaggio di allerta in modo da notificare il malfunzionamento di un nodo edge e comunicare i suoi dati. (E)

### Lato watchdoge:

* Come sentinella, voglio poter generare dei dati fittizi in modo da simulare una rilevazione di dati da parte di sensori.
* Come sentinella, voglio poter simulare diversi stati di funzionamento in modo da simulare un dispositivo elettronico fisico.

## Use Case Diagram



## Deployment Diagram

Lo scopo di questa fase è quello di realizzare un Deployment diagram, ossia un diagramma che ha il compito di rappresentare la vista statica delle componenti della rete, in altre parole si vogliono descrivere le parti hardware della rete e le relazioni tra esse. In un primo momento abbiamo optato per un diagramma informale, che non segue alcuna regola di raffigurazione ma aiuta a inquadrare l’idea del progetto.

In un secondo momento abbiamo seguito i principi del Deployment Diagram UML che , oltre a raffigurare la parte hardware del sistema, sottolinea anche il software che gira su una determinata componente.

### Deployment Diagram Informale

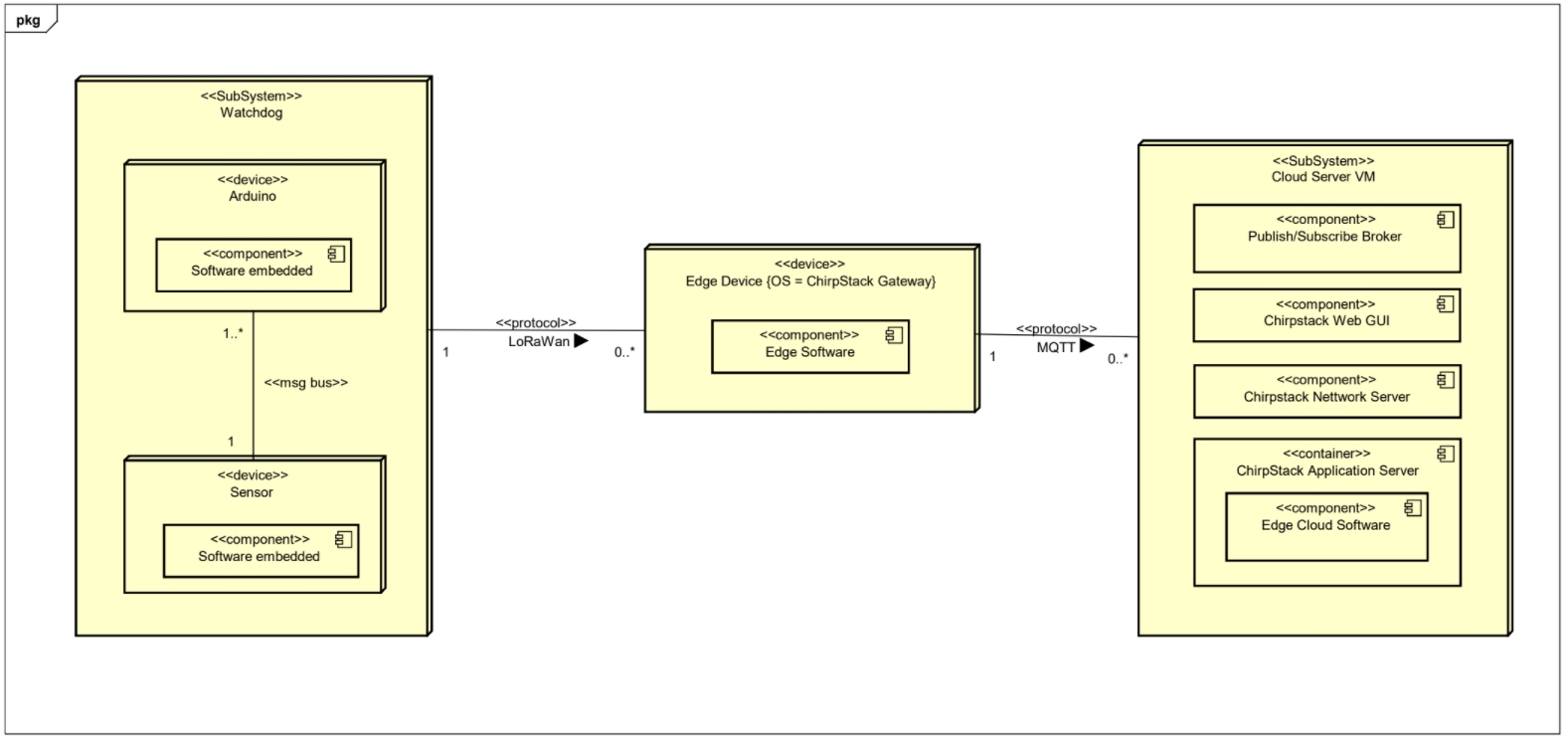
Nel seguente diagramma sono rappresentati gli attori della rete : *watchdog, edge device* e la *cloud virtual machine*. Inoltre, sono ritratte le aree dove risiedono le parti hardware. L’area di acquisizione contiene sia watchdog che edge device, sappiamo che la comunicazione tra essi avviene tramite protocollo LoRaWan e che un edge device riceve messaggi da più watchdog. I messaggi scambiati tra la rete di acquisizione e la *cloud virtual machine* avvengono tramite il protocolloMQTT che abbiamo espresso come un canale di comunicazione. Le client application sono tutte quelle applicazioni che possono interagire con le server application.



### Deployment Diagram UML

Nel deployment diagram UML sono definiti tre *Subsystem* principali:

* Watchdog: questo sottosistema contiene due *device* hardware, un microcontrollore Arduino e i relativi sensori. Si può notare che un Arduino può avere uno o più sensori (per esempio di umidità, temperatura, CO2 ecc..), mentre un sensore può interfacciarsi ad uno e un solo microcontrollore. Su entrambi i dispositivi girano dei componenti software embedded, che noi simuleremo successivamente con la tecnica del *digital twin,* discussa nel capitolo introduttivo.
* Edge-device: tale sottosistema comunica con il watchdog attraverso il protocollo LoRaWan e con il cloud server VM per mezzo del protocollo MQTT. Un edge device riceve messaggi da zero (caso estremo) a molti watchdog e li inoltra ad uno e un solo cloud server VM. Il sistema operativo installato su questo dispositivo sarà verosimilmente il *Chirpstack gateway,* uno strumento messo a disposizione da Chirpstack per semplificare le operazioni di configurazione del gateway. Anche in questo caso sfrutteremo la tecnica del *digital twin*.
* Cloud Server: questo sottosistema comunica con zero(caso estremo) a molti edge device. Abbiamo deciso di esplodere alcune componenti software indicate da Chirpstack, quali il broker mqtt, il network server, l’application server e l’interfaccia grafica.



# Iterazione 1

Installazione dello stack Chirpstack su macchina virtuale Ubuntu e set up dell'ambiente di lavoro.

# Iterazione 2

Implementazione del funzionamento di un edgenode e simulazione.

Questo comprende dettagliare la componente EdgeNodeSoftware

# Iterazione 3

Implementazione del funzionamento di un watchdog e simulazione di quest'ultimo.

Questo viene fatto dettagliando la componente WatchdogSoftware

# Iterazione 4

Introduzione AppServer con implementazione requisito R0.

Questo comprende il dettaglio della componente EdgeCloudSoftware e l'introduzione di un mapek-loop per

il l'adaptation goal della configurazione per allungare il ciclo di vita dei watchdog

# Iterazione 5

Implementazione requisito R1. Questo comprende l'introduzione di un mapek-loop per

la diagnosi dei guasti.