Intelligent Internet of Things
Proposta Progettuale

Scenario Applicativo

Intrusion Detection System Fisico / Security System

Studenti

Edoardo Torrini 152652 287357@studenti.unimore.it

Descrizione

L'obiettivo del progetto e' la realizzazione di un sistema IoT che coinvolga i seguenti dispositivi (sensori e attuatori):

Nome	**Tipologia**	**Descrizione**
People Counter Smart Object	Sensor	Smart Object ad un sensore di presenza: va a definire il numero di persone che entrano e quelle che escono, in modo tale da avere un controllo sul numero di persone presenti all'interno di una stanza, pensato principalmente per un locale server di un'azienda/ente
Light Controller Smart Object	Actuator	Smart Object che permette l'accensione e lo spegnimento della luce all'interno del locale, in base al numero di persone presenti
Alarm Controller Smart Object	Actuator	Smart Object per regolare l'accensione dell'allarme in caso di forzatura o tentative di intrusione all'interno del locale
Door Lock Smart Object	Sensor Actuator	Smart Object che ha funzionamenti sia da sensore che da attuatore: ● Sensor: permette la lettura di un'impronta digitale al quale è collegato un token necessario per l'autenticazione all'ingresso ● Sensor: permette la lettura dell'accellerazione applicata alla serratura, in modo da poter intervenire in caso di cercata manomissione ● Sensor: permette la lettura dello stato della porta, ovvero se la porta è aperta o chiusa in base allo stato dei due magneti della serratura, se sono allineati allora la porta è chiusa, se no aperta ● Actuator: permette lo sblocco della serratura
Environmental Monitoring Smart Object	Sensor Actuator	Smart Object per la gestione degli allarmi legati all'ambiente, può funzionare sia da sensore che da attuatore: ● Sensor: telemetria sui dati ambientali, quali: temperature, umidità, indice UV, Fumo ● Actuator: in base a cosa viene riconosciuto è possibile aumentare o diminuire il livello della temperature all'interno della sala, attivare o meno il deumidificatore e gestire casi di fire detection o flooding detection

Specificare se il progetto sviluppato dovra' essere progettato per supportare ***n*** dispositivi per ogni tipologia in funzione dello scenario applicativo (ovviamente in fase di demo del progetto e' possibile emulare il numero minimo di device per mostrare il corretto funzionamento del sistema sviluppato).

Nell'architettura sarà presente anche un **Data Collector & Manager** capace di ricevere i dati di tutti i device coinvolti e implementare i seguenti comportamenti

- Su ogni porta, sarà presente un **Door Lock Smart Object** che verrà gestito tramite i dati ricevuti, quali: l'impronta digitale che permetterà lo sblocco della porta, o in caso di **Brute Force Attack**, l'attivazione di un allarme, come anche nel caso di un tentavo di forzatura della serratura tramite l'accellerometro presente sul dispositivo.
- All'interno di ogni **Room** sarà presente un **Environmental Monitoring Smart Object** che permetterà il logging dello stato dell'ambiente all'interno della sala server, e di possibili **policy** di **Disaster Recovery**

Policy:

- **Disaster Recovery:**
  - Umidità in lettura compresa tra il 60 e l'80% viene acceso il deumidificatore per evitare il deterioramento dei server, se l'umidità percepita sul pavimento è maggiore dell'80% allora è in corso un allagamento e verrà inviato un messaggio di **flooding detection**
  - Temperatura percepita compresa tra i 25-30°C attivazione del condizionamento a bassa spinta, 30-35°C attivazione del condizionamento a media spinta, 35-40°C attivazione del condizionamento ad alta spinta
  - In caso di variazione nell'indice Uv e del Fumo percepito, viene inviato un messaggio di **fire detection**

- **Intrusion Detection System:**
  - Nel caso in cui l'accellerazione della serratura vada sopra una certa soglia e non viene eseguito un accesso tramite impronta digitale entro un certo tempo **t** allora si considera come forzatura della serratura e viene inviato un **tentativo** di **intrusione**
  - Nel caso in cui venga eseguito un ingresso senza una mancata identificazione all'interno di un certo periodo di tempo **Δt,** allora si presuppone che sia stato violato l'accesso e si manda un allarme di **intrusione**
  - Nel caso in cui vengano eseguiti troppi tentativi di accesso dal lettore di impronte digitali all'interno di un **Δt** allora si presuppone che sia in atto un **brute force attack** e si manda un allarme di **tentativo** di **intrusione**