

UNIVERSITÀ DEGLI STUDI DI MILANO
Facoltà di Scienze e Tecnologie
Corso di Laurea in Informatica

Sistema Accessi IoT

Relatore: Dott. Andrea TRENTINI

Correlatore: Marco LANZA

TESI DI LAUREA DI:

Andrei CIULPAN

Mat. 872394

Anno Accademico 2018/2019

Ringrazio i miei genitori e la nonna per il sostegno e per la pazienza che hanno avuto.

Ringrazio i miei amici e compagni di università per aver reso l'esperienza più bella e soprattutto più facile.

Ringrazio i miei tutor e colleghi per avermi dato la possibilità di crescere e concludere la mia esperienza universitaria.

Un ringraziamento speciale a Elena per essere riuscita a farmi sorridere e a tirarmi su il morale in ogni giorno con la sua presenza nella mia vita. Un altro ringraziamento a lei per la revisione della tesi.

Indice

1	Introduzione	1
1.1	Panoramica del progetto	2
2	Hardware	4
2.1	Raspberry Pi	4
2.2	Arduino UNO	4
2.3	RTC (perchè la Raspberry Pi non ce l'ha ed è privo di connessione Internet)	4
2.4	Ricevitore RF	4
2.5	Servomotore	4
2.6	RFID	5
2.7	Display LCD 16x2	5
2.8	Keypad	5
2.9	ESP-01	5
2.10	Protocolli di trasmissione dati	5
2.10.1	Logica IoT	5
2.10.2	Comunicazione Wi-Fi in rete locale. Parlo anche del protocollo HTTP?	5
2.10.3	I2C	5
2.10.4	SPI	5
3	Software	6
3.1	Strumenti dello sviluppatore	6
3.2	Sviluppo del sistema embedded	6
3.3	Sviluppo dell'interfaccia web	6
3.3.1	Back-End	6
3.3.2	Front-End	7
4	Analisi del progetto	8
5	Conclusioni	9

Capitolo 1

Introduzione

Il controllo accessi è un sistema di protezione che permette l'accesso solo a determinate persone per via di qualche procedura di autenticazione: nel mondo fisico si può parlare di una semplice serratura (storicamente il sistema più utilizzato in assoluto) che può essere aperta solo dalle persone in possesso della chiave, mentre nel mondo dell'informatica si può notare l'enorme utilizzo delle procedure di autenticazione (login) che aiutano il sistema, tramite l'inserimento di un nome utente e password, a determinare automaticamente se una persona è autorizzata ad accedere alle risorse del sistema stesso.

Il controllo accessi[1] è un tema molto sviluppato nel campo della sicurezza sia fisica che informatica: è stato segnalato che nel 2017, per il secondo anno consecutivo, il mercato del controllo accessi ha avuto la crescita più rapida nell'industria della sicurezza fisica[2]. E' anche un sistema onnipresente, utilizzato in ospedali, fabbriche, supermercati, aziende, sistemi di trasporto pubblico (e.g l'ATM di Milano), case e tanti altri campi.

La tesi si propone di trattare un sistema ibrido in cui il mondo fisico e il mondo informatico lavorano insieme: attraverso sensori ed attuatori è possibile avere la comunicazione tra i due mondi. Si tratta di un sistema IoT (Internet of Things), ovvero un sistema in cui la connessione Internet viene estesa anche al mondo degli oggetti fisici (smart objects[3]) di uso comune. Gli oggetti si rendono riconoscibili e acquisiscono intelligenza grazie al fatto di possedere una o più delle seguenti funzionalità: identificazione, localizzazione, diagnosi di stato, interazione con l'ambiente circostante, elaborazione dati e ovviamente connessione. Gli oggetti intelligenti di un sistema IoT sono normalmente dotati di un processore embedded, sensori e attuatori e sono in grado di agire sui dati raccolti dall'ambiente e, ancora più importante, mandare questi dati in rete dove possono poi essere analizzati[4]. Un semplice esempio di un sistema IoT si può trovare in Figura 1.

Le seguenti sezioni di questo capitolo introdurranno il progetto stesso (denominato

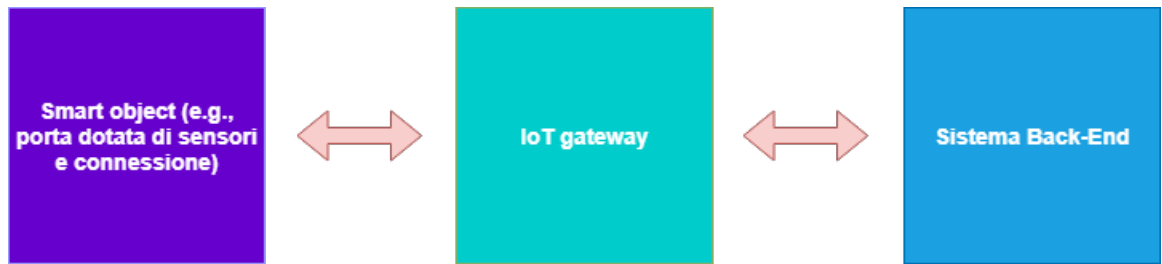


Figura 1: Esempio di sistema IoT

SimSim) che poi verrà dettagliato nei prossimi capitoli.

1.1 Panoramica del progetto

L'attività principale del tirocinio è la realizzazione di un sistema di controllo accessi basato su Arduino, da applicare presso varchi. Il sistema è in grado di funzionare con diverse modalità di riconoscimento quali RFID, controllo remoto e tastierino numerico. A seguito di ogni accesso avvenuto con successo, il sistema salva il log in un database remoto (in LAN) via WiFi.

Parallelamente il sistema possiede un'interfaccia per l'utente utilizzatore (in questo caso un sito web) dove può accedere ai log degli accessi, oltre a un database per poter gestire i soci e le tessere RFID dell'azienda. Il server web è sviluppato utilizzando NodeJS e MongoDB (per il database) ed è hostato su un Raspberry Pi 3B+.

Nelle figure 2 e 3 si possono trovare rispettivamente un diagramma dei casi d'uso e un diagramma di flusso del sistema.

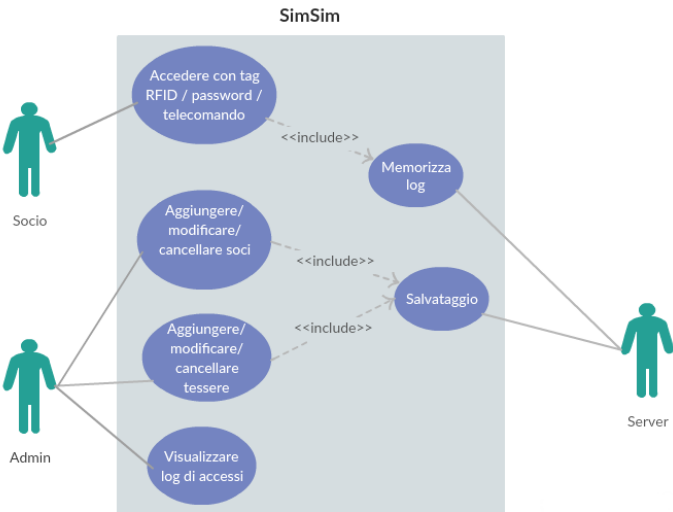


Figura 2: Casi d’uso del sistema

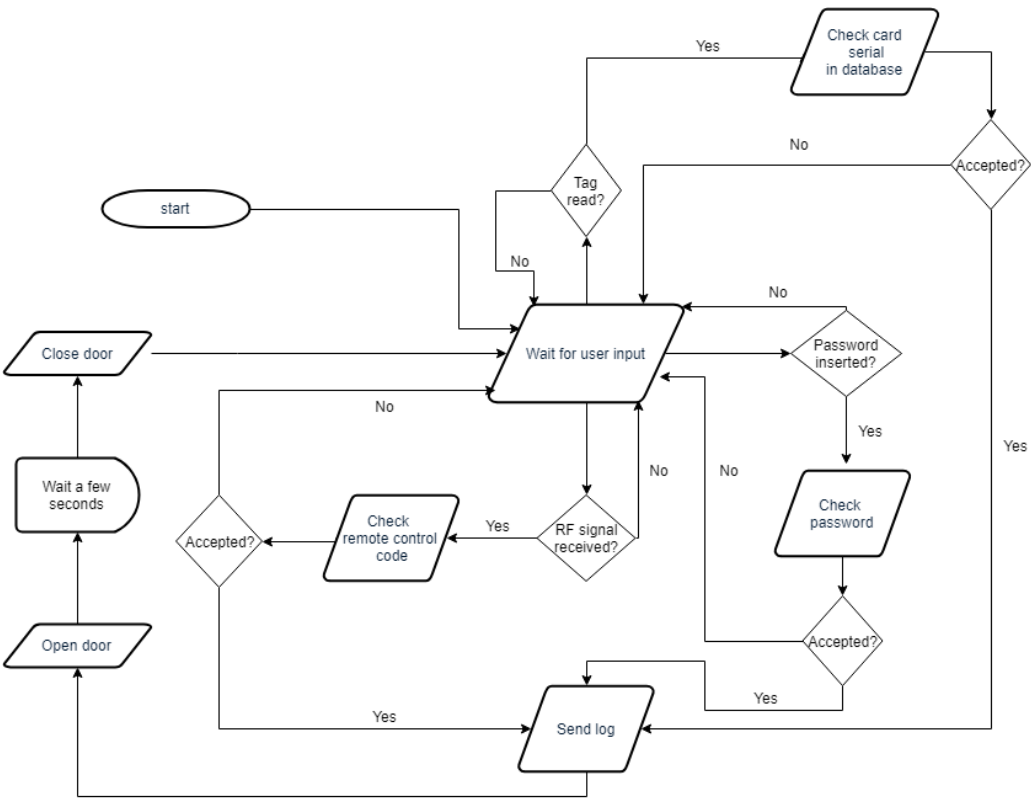


Figura 3: Diagramma di flusso del sistema

Capitolo 2

Hardware

Schema circuitale completo?

2.1 Raspberry Pi

2.2 Arduino UNO

2.3 RTC (perchè la Raspberry Pi non ce l'ha ed è privo di connessione Internet)

2.4 Ricevitore RF

Un po' di matematica sulle antenne

2.5 Servomotore

PWM

2.6 RFID

2.7 Display LCD 16x2

2.8 Keypad

2.9 ESP-01

Problematiche

Alternative

2.10 Protocolli di trasmissione dati

2.10.1 Logica IoT

2.10.2 Comunicazione Wi-Fi in rete locale. Parlo anche del protocollo HTTP?

2.10.3 I2C

2.10.4 SPI

Capitolo 3

Software

3.1 Strumenti dello sviluppatore

Arduino IDE

Node.js

Postman

MongoDB

Per i linguaggi di programmazione metto solo un riferimento alla bibliografia

3.2 Sviluppo del sistema embedded

Snippet e spiegazioni di codice

3.3 Sviluppo dell'interfaccia web

3.3.1 Back-End

Scelte progettuali

MVC

Database

API

Documentazione delle API del back-end

3.3.2 Front-End

Scelte progettuali

Le basi: Javascript, HTML5 & CSS

w3.css

jQuery

EJS

Capitolo 4

Analisi del progetto

Prestazioni

Problema sicurezza

Possibili miglioramenti

Capitolo 5

Conclusioni

Appendice A

Una prima Appendice (?)

...

Sitografia

- [1] J. Allen, Opening new doors with IP access control, 16 Marzo, 2018. <https://www.axis.com/blog/secure-insights/opening-new-doors-with-ip-access-control/>
- [2] R. Alalouff, Access control leads growth in physical security market but video surveillance still dominates, 25 Gennaio, 2018. <https://www.ifsecglobal.com/access-control/access-control-leads-growth-physical-security-market-video-surveillance-still-dominates/>
- [3] A. Tumino, Internet of Things: gli oggetti intelligenti prima di ogni "cosa", 24 Gennaio, 2018. https://blog.osservatori.net/it_it/internet-of-things-oggetti-intelligenti-prima-di-ogni-cosa
- [4] M. Rouse, Internet of Things (IoT), ultimo aggiornamento Marzo 2019. <https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT>