Analisi e implementazione di una soluzione per mutua autenticazione in ambito IoT device embedded

Tesi di Laurea Triennale in Ingegneria Informatica

Candidato: Samuele Meta
Relatore: Prof. Paolo Nesi
Correlatore: Ing. Angelo Difino

Università degli Studi di Firenze
Dipartimento di Ingegneria dell'Informazione
Anno Accademico 2017-2018

Internet of Things - Calcolatori

Con il termine **Internet of Things** si fa riferimento a un sistema di interconnessione tra calcolatori, oggetti, animali o persone a cui è stato fornito un univoco identificativo e la capacità di trasferire dati sulla rete.

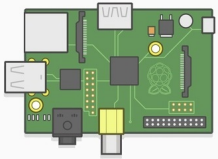
Desktop

Tablet

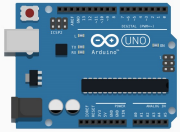
Mobile

Internet of Things - Oggetti

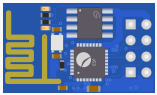
Con il termine **Internet of Things** si fa riferimento a un sistema di interconnessione tra calcolatori, oggetti, animali o persone a cui è stato fornito un univoco identificativo e la capacità di trasferire dati sulla rete.



Raspberry Pi



Arduino

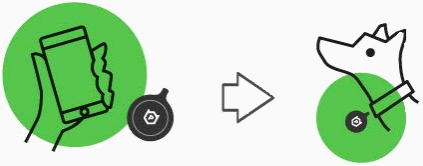


ESP8266

Internet of Things - Persone e Animali

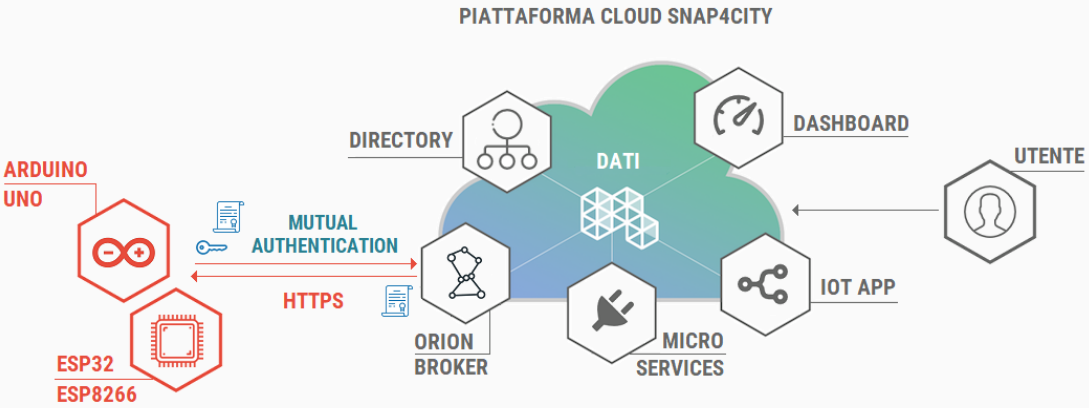
Con il termine **Internet of Things** si fa riferimento a un sistema di interconnessione tra calcolatori, oggetti, animali o persone a cui è stato fornito un univoco identificativo e la capacità di trasferire dati sulla rete.

Smart Watch



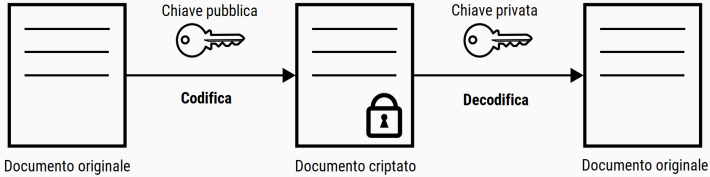
Collare con tracciamento GPS

Piattaforma Cloud Snap4City



Chiavi

La crittografia asimmetrica implementa un approccio in cui, ad ogni attore coinvolto nella comunicazione, viene assegnata una coppia di chiavi. Queste sono dette **pubblica** e **privata**.



Certificato

```
MIIFmTCCA4GgA
wIBAgIBCDANBg
Bgkqhk
ELMAkG
AgTCEZ
```

- Versione
- Ente
- Validità
- Algoritmi

- Chiave
- Soggetto
- Firma

Lato server è stato generato servendosi di una chiave a **2048** bit.

Lato client è stato generato avvalendosi di una chiave a **1024** bit.

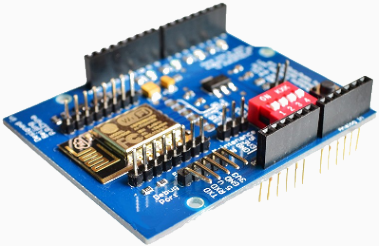
Caratteristiche Hardware - Arduino ed ESP8266

ARDUINO UNO

Microcontrollore: **ATmega328P**

Pin: **14** digitali e **6** analogici

Memoria: **32 KB**



SHIELD WIFI ESP8266

Processore: **Tensilica Xtensa 106**

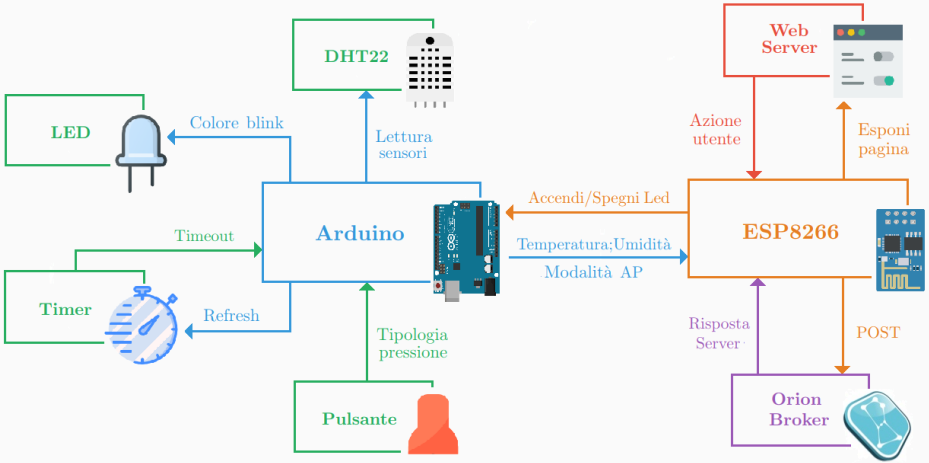
Memoria istruzioni: 32 KiB

Memoria dati: 96 KiB

Soluzioni software - Arduino ed ESP8266

- Dimensionamento di chiave e certificato (memoria non volatile)
- Riduzione dell'utilizzo del tipo `String`
- Specifiche impostazioni di compilazione (circa 3 KiB)

Scenario di interesse



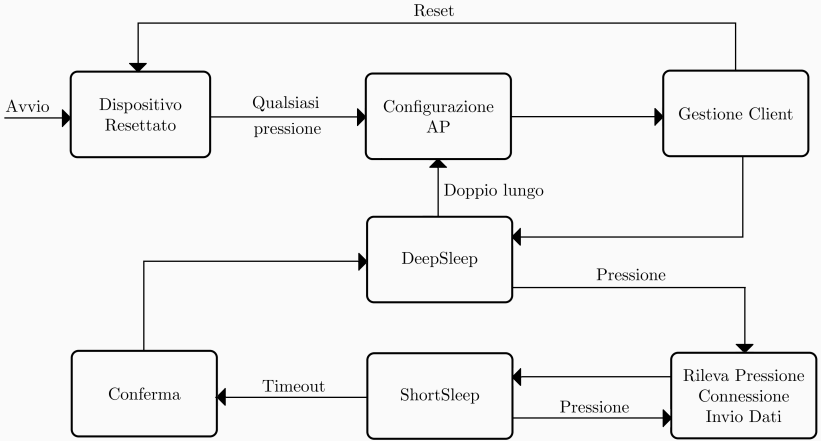
Caratteristiche Hardware - IoT Button

Chip: **ESP32**
Processore: **Tensilica Xtensa LX6**
Memoria: **520 KiB**
Alimentazione: 3V
Cryptographic hardware acceleration

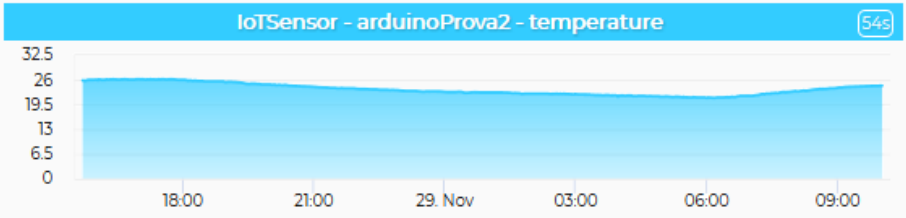
Soluzioni software - IoT Button

- Riduzione delle tonalità del LED
- Riduzione della potenza trasmissiva in modalità setup
- Ristrutturazione del codice secondo una macchina a stati

Scenario di interesse

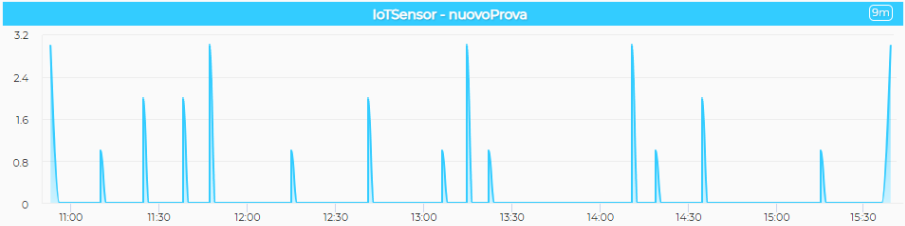


Dashboard Temperatura



Andamento temporale delle misurazioni della temperatura operate dal sensore.

Dashboard Impulsi

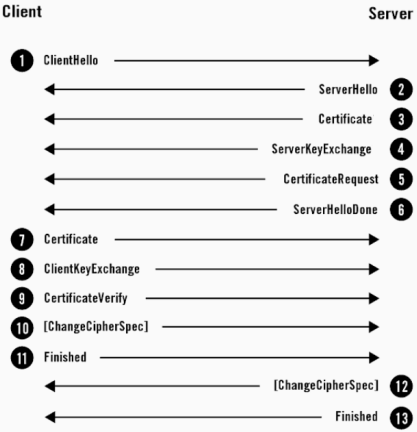


Andamento temporale dei segnali recapitati alla piattaforma.

A ogni ampiezza corrisponde una specifica tipologia di pressione.

Backup

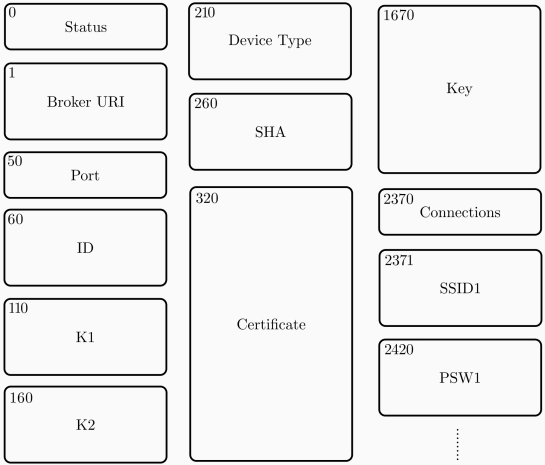
TLS


Client
Server
1 ClientHello
ServerHello 2
Certificate 3
ServerKeyExchange 4
CertificateRequest 5
ServerHelloDone 6
7 Certificate
8 ClientKeyExchange
9 CertificateVerify
10 [ChangeCipherSpec]
11 Finished
[ChangeCipherSpec] 12
Finished 13

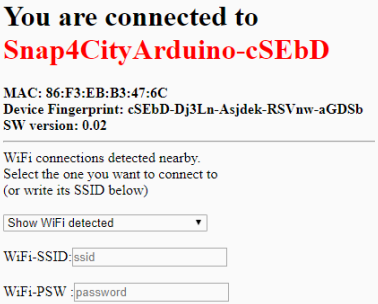
HTTPS POST

```
{ "contextElements": [ {
   "type": "Ambiental",
   "isPattern": false,
   "id": "myArduino",
   "attributes": [ {
     "name": "temperature",
     "type": "float",
     "value": "23"
    }, {
     "name": "humidity",
     "type": "float",
     "value": "72"
    } ] } ],
 "updateAction": "APPEND" }
```

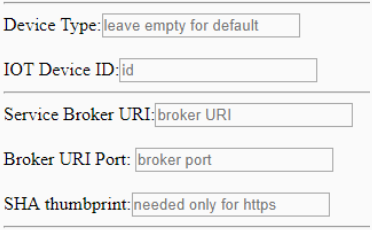
EEPROM


0
Status
1
Broker URI
50
Port
60
ID
110
K1
160
K2
210
Device Type
260
SHA
320
Certificate
1670
Key
2370
Connections
2371
SSID1
2420
PSW1

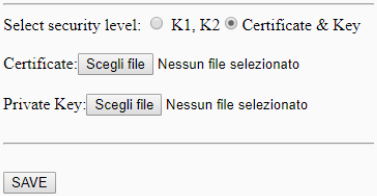
WEBSERVER


You are connected to
Snap4CityArduino-cSEbD
MAC: 86:F3:EB:B3:47:6C
Device Fingerprint: cSEbD-Dj3Ln-Asjdek-RSVnw-aGDSb
SW version: 0.02
WiFi connections detected nearby.
Select the one you want to connect to
(or write its SSID below)
Show WiFi detected
WiFi-SSID:ssid
WiFi-PSW :password

WEBSERVER


Device Type:
leave empty for default
IOT Device ID:
id
Service Broker URI:
broker URI
Broker URI Port:
broker port
SHA thumbprint:
needed only for https

WEBSERVER


Select security level: K1, K2 Certificate & Key
Certificate: Scegli file Nessun file selezionato
Private Key: Scegli file Nessun file selezionato
SAVE