SMASHBOX

**FUNZIONAMENTO GENERALE:**

SMASHBOX è un sistema che simula l’utilizzo delle classiche cassette di sicurezza della banca in modo più accessibile e smart rispetto allo scenario attuale.

Si compone di un N cassette di sicurezza (chiamate ACQUISITION) (il nostro prototipo ne comprende 2) e di una supplementare che funge da controllo per le altre (chiamata CENTRAL).

Ogni cassetta di sicurezza può essere registrata da un cliente tramite l’impronta digitale della mano, in modo da avere una chiave univoca e personale. Ogni cassetta ha la possibilità di tracciare lo stato interno della cassetta con dei parametri come temperatura, umidità, verificare se la cassetta è aperta o meno e se c’è stata una tentata manomissione. Il monitoring di questi parametri è utile per notificare il cliente in caso di tentativo di furto (manomissione) o di pericolo (aumento temperatura). Inoltre viene fornito un log con le diverse date e orari di apertura.

La notifica dei log e degli allarmi sfrutta un bot Telegram che viene registrato nel momento in cui il cliente acquista la possibilità di utilizzare una cassetta.

In caso di allarme il sistema si mette in quella che viene definita “SAFE-MODE”, ovvero tutte le cassette vengono bloccate, e solo un operatore può effettuare lo sblocco tramite un pulsante dedicato presente sul CENTRAL.

(FOTO SMASHBOX)

# MACRO COMPONENTI software

1. **LOCAL**: parte di acquisizione dei dati di monitoring e spedizione verso il BRIDGE.
2. **BRIDGE**: parte di recupero e inoltro verso il CLOUD.
3. **CLOUD**: gestione in cloud dei Digital Twin.
4. **CLIENT**: agenti esterni che possono accedere al CLOUD tramite interfaccia

# DETTAGLIO COMPONENTI

**LOCAL**

Questa sezione è divisa in due parti:

* Acquisition: la board scelta per leggere i dati dai sensori. Gestisce strettamente l’acquisizione dei dati dai sensori e l’inoltro tramite un canale (seriale o Wi-Fi) verso il Bridge.
* Central: Un Arduino dedicato gestisce il riconoscimento dell’impronta digitale. Centralizzata perché ci sarà un unico riconoscitore per tutte le cassette.

**ACQUISITION**

Questo componente è composto da

* Arduino
* Sensore di temperatura e umidità (Adafruit\_AHTX0)
* Accelerometro (ADXL345)
* 2 sensori di presenza (sportello e presenza oggetto)
* Un elettromagnete sostiene il blocco dello sportello quando è in modalità lock.

**CENTRAL:**

L’altra parte del LOCAL, quella centralizzata che effettua sia le registrazioni che le richieste di sblocco da parte dell’utente.

Questa è composta da:

* Sensore di impronte (Adafruit\_Fingerprint)
* Display di servizio
* Un pulsante per resettare la safe-mode (v. dopo)

**BRIDGE**

Il Bridge è uno script Python che ha due endpoint che lavorano in sinergia: uno lato LOCAL e uno lato CLOUD. L’idea di base è che il BRIDGE passi continuamente i dati che arrivano da LOCAL verso CLOUD (e viceversa). Il pacchetto di monitoring arriverà in un'unica trasmissione gestita da un protocollo (v. dopo). Il BRIDGE spacchetta tramite un Parser i dati ed effettua i comandi di update (HTTP/MQTT) verso il CLOUD in maniera separata.

Il BRIDGE è anche il punto di comunicazione tra CENTRAL e le varie ACQUISITIONS, dal momento che ci sono casi in cui il CENTRAL deve comunicare un informazione alle possibili N boards che sono le varie cassette.

**CLOUD (THINGSBOARD)**

La piattaforma scelta per il Cloud è Thingsboard. Qui avverrà il monitoring dei dati nel corrispondente Digital Twin e la gestione dei trigger scaturiti sulla base dei dati che arrivano dal Bridge.

Sostanzialmente raccoglie di ogni cassetta e comunica a tutte le altre di intervenire in caso di Safe Mode.

**TELEGRAM BOT**

E’ un endpoint in cui l’utente viene notificato di aperture della propria cassetta, di eventuali allarmi. Inoltre viene data la possibilità al cliente tramite comando al bot di capire quali sono stati i vari log della propria cassetta registrata.

***/\* MQTT SERVER(MQTT)***

*C’è un ulteriore blocco, che sarà un broker MQTT sul server dove appoggiarsi per scambiare dati tra BRIDGE e THINGS. L’idea è che i trigger di allarme siano mandati su questo server (test.mosquitto.org) e recuperati dal BRIDGE sullo stesso. Questo perché Thingsboard nella sua versione free possiede soltanto la versione per scambiare i dati verso il server e non dal server.*

***SERVER CUSTOMERS (FIREBASE)***

*L’idea di accedere ad un server per visualizzare il log e di poter sottoscrivere per una nuova cassetta potrebbe essere fatta tramite una app che fa delle richieste ad un Server dedicato in cui sono contenuti i log delle cassette. Lo stesso server contiene anche la lista dei clienti registrati che tentano di accedere allo sblocco. Questo non solo può essere usato per il log, ma anche come backup dei clienti registrati sul central per accedere alle cassette. Tutto questo sarà gestito con un Real Time Database di Firebase.*

*Lo schema generale potrebbe essere quello linkato al repository: \Doc\Blocks \*/*

# FUNZIONAMENTO

Il sistema nel prototipo è composto da due cassette di sicurezza (ACQUISITION), e una cassetta centralizzata (CENTRAL), un bridge (script Python) e un bot Telegram.

3.1 INIT

Allo startup, ACQ si mette in attesa del BRIDGE, mentre CNRTL manda sulla seriale un pacchetto identificativo (7 byte) di tutti 0 e si mette in attesa del BRIDGE stesso.

uint8\_t idle\_packet\_init[PACKET\_SIZE] = {0,0,0,0,0,0,0};

Il BRIDGE, una volta lanciato, scannerizza tutte le seriali e legge da ognuna. Quando legge il pacchetto identificativo di CRNTL divide in una lista le seriali collegate a ACQ e l’altra legata a CNTRL.

A questo punto, la parte CNTRL che era in attesa viene risvegliata dal bridge tramite l’invio sulla seriale (dedicata a central) un carattere identificativo per procedere. Le ACQ restano ancora in attesa.

Quello che stanno attendendo è l’ID. Poiché si sta simulando il primo power on del sistema, le cassette fin quando non sono registrate, non possono partire. E per partire hanno bisogno di un ID.

Il CNTRL, risvegliato, entra in fase di enroll, dove aspetta due registrazioni (come le cassette del sistema). Si simula a questo punto la registrazione di due dita (che simulano diversi clienti). Ogni volta che viene registrata una cassetta, da CNTRL viene inviato un pacchetto con l’ID verso il bridge (2 byte), uno identifica l’header (PACKET\_ENROLL) e l’altro byte l’ID stesso.

Il bridge riceve questo pacchetto con l’ID, lo estrae e la manda ad una delle box non già registrate (questo viene tracciata in un dizionario python). Il pacchetto che viene inviato in questo caso sono 10 byte con il meno significativo contenente l’ID. L’ACQ nella sua attesa legge 10 byte sulla serial e quando li riceve (grazie all’enroll) assegna l’ID alla cassetta ed entra in loop.

Nel mentre viene ripetuta la seconda registrazione dell’impronta in modo da replicare lo stesso processo per la cassetta non ancora registrata.

Immagine che contiene testo, schermata, Carattere, numero

Il contenuto generato dall'IA potrebbe non essere corretto.

3.2 SAFE MODE

Le cassette e il CNTRL funzionano in due modalità

* IDLE (funzionamento normale)
* SAFE MODE (caso di allarme)

Il secondo caso viene triggerato dal server: quando i dati di ACQ giungono al server, questi vengono controllati. In particolare, se viene effettuata una manomissione (accelerometro mosso) oppure temperatura e umidità superano alcune soglie, tramite un messaggio MQTT viene inviato al BRIDGE che lo raccoglie e questo notifica la parte local: sia CNTRL che ACQ. La prima si mette in modalità SAFE MODE da cui si può uscire soltanto con una operazione manuale da parte di un operatore (simulato con un push button sul retro). Le seconde entrano anch’esse in modalità SAFE MODE (led lampeggianti) in cui il pacchetto viene riempito da tutti 0 tranne il Lock.

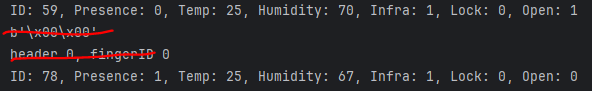
Un messaggio di allarme viene inviato anche al BOTTG.

3.3 ACQUISITION

Una volta che il CNTRL ha assegnato l’ID, ogni singola ACQ prende i dati dai sensori

* Temperatura + Umidità
* Accelerometro
* Presenza oggetto
* Rilevamento sportello aperto o no

Se in modalità IDLE (e quindi non in SAFE MODE) Tutti questi dati vengono mandati ad ogni ciclo al bridge in un pacchetto di 7 byte.



Altrimenti, SAFE MODE vuol dire che il pacchetto sarà costituito da 7 byte, ma tutti a 0 tranne il lock uguale a 1.



3.4 FINGERPRINT MODE (CHECK)

A questo punto Central aspetta che qualcuno voglia sbloccare le cassette tramite il riconoscimento di un impronta digitale. Una volta appoggiato il dito sul sensore, la cassetta verrà sbloccata sulla base di quale dito è stato registrato (ricordando che ogni dito simula un cliente di una cassetta).

Una volta sbloccata, una cassetta si apre e il LED assegnato a tale cassetta è acceso. Si può simulare la presenza dell’oggetto inserendo al proprio interno un ostacolo da rilevare. La cassetta va aperta (sensore di apertura riconosce che lo sportello è stato aperto solo se è molto aperto) a questo punto il magnete si riattiva, pronto per la richiusura.

3.1 VALID AUTH

Nel primo caso il BRIDGE legge la risposta che sarà composta da una coppia (ID\_CLIENTE + NUMERO CASSETTA) e manda l’update al CENTRAL. Se esiste il cliente, CENTRAL attende il feedback della camera per verificare che effettivamente c’è corrispondenza tra cliente e numero. Lato ACQUISITION, BRIDGE manderà lo sblocco solo alla cassetta associata con l’ID(ACQUISITION\_X). Lo sblocco può essere soltanto fatto dal BRIDGE, l’utente non può (altrimenti rientriamo in manomissione). Lato THINGS deve aggiornare lo stato del Digital Twin in maniera che sia notificato il fatto che sia aperta.

Quando termina l’operazione e quindi la chiusura manuale, ACQUISITON\_X manda un feedback di avvenuta chiusura (tramite sensore di luce?), BRIDGE aggiorna CENTRAL (che torna in stato IDLE) e THINGS.

3.2 INVALID AUTH

Nel secondo caso, se viene negato l’autorizzazione BRIDGE manda a CENTRAL un errore e viene notificato e torna in IDLE. ACQUISITION non viene coinvolto.

3.3 SAFE MODE

Lo stato di monitoring deve essere sempre attivo. ACQUISITION deve continuamente mandare i dati ogni x secondi (TBD quanti). BRIDGE spacchetta i dati e aggiorna i campi su THINGS. Se viene superata una qualsiasi soglia si entra in *SafeMode*.

Quando viene innescata, viene inviato un messaggio MQTT su un server esterno (MQTT) che viene prelevato dal bridge. A questo punto, le cassette devono entrare in lock e non possono essere aperte. L’innesco provoca un inoltro del comando ricevuto da BRIDGE verso CENTRAL (in stato PROTECTION o BUSY in modo che non avvenga nessuna identificazione su FINGERPRINT) e verso tutte le ACQUISITION, che devono essere lockate. Si esce da questa modalità solo un uno sblocco su CENTRAL (pulsante manuale ad esempio). Lo sblocco manuale da CENTRAL (stato IDLE a quel punto) manda una notifica a BRIDGE che sblocca la possibilità di essere aperte tutte le ACQUISITION. Automaticamente, aggiornando lo stato delle acquisition, thingsboard si aggiornerà in automatico.

# PROTOCOLLO ACQUISITION -> BRIDGE

L’idea è di mandare un pacchetto unico di dati che comunichi tutto il monitoring. I vari campi potrebbero avere tipi di dato diversi (anche per più blocchi)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **START BYTE 0x1D** | **Temperature** | **Accel** | **Presence** | **Lock (1byte)** | **END BYTE**  **0xFF** |

/\* TODO: Aggiungere qui la descrizione di cosa si riceve dai vari sensori, come viene acquisito e tutto quello che serve da descrivere \*/

# CLIENT