Documentazione

PassChain IoT

Riferimento	
Versione	1.0
Data	15/05/2022
Destinatario	Prof. P. Ritrovato Prof.ssa L. Fotia
Presentato da	Montefusco Alberto Spina Gennaro Oskar Szuba

Sommario

1. Introduzione

1.1 Scopo del Sistema

La realizzazione di PassChain ha come obiettivo quello di facilitare l'utente nell'autenticazione digitale ma anche di assicurare la sicurezza attraverso la sua funzione di password manager. Con questo sistema l'utente non dovrà fare altro che collegarlo ad un dispositivo (Computer, Smartphone, …) tramite Bluetooth e, una volta che si è autenticato tramite un tastierino numerico, le credenziali scelte saranno inviate automaticamente nei campi che l'utente ha selezionato per la verifica. Quindi, tra gli obiettivi che il sistema propone di assicurare abbiamo: la sicurezza, l'efficienza, la portabilità e la versatilità.

1.2 Panoramica

Nei seguenti capitoli andremo ad analizzare i requisiti funzionali e non funzionali che il sistema deve necessariamente assicurare (Capitolo 2). Inoltre, verranno descritti gli strumenti Software utilizzati per la realizzazione dell'interfaccia grafica che permette il setup del sistema IoT da parte dell'utente, i dispositivi Hardware aggiuntivi integrati nella scheda ESP32 ed i linguaggi utilizzati per la programmazione IoT (Capitolo 3).

2. Sistema Proposto

Il sistema che proponiamo di realizzare è un dispositivo IoT che permette ad un utente di autenticarsi in un sito web oppure in un'applicazione per smartphone in pochi e semplici passi, inoltre, l'utente non dovrà ricordare tutte le password e gli username che possiede poiché PassChain funge anche da password manager: al suo interno saranno memorizzate un insieme di credenziali (cifrate) che l'utente potrà reperire tramite semplici steps.

Spieghiamo ora il funzionamento del sistema proposto. All'accensione, l'utente visualizzerà, su un piccolo schermo LCD, una scritta di benvenuto e sentirà un piccolo suono seguito da un primo tentativo di connessione ad un dispositivo tramite Bluetooth. Una volta che PassChain si sarà collegato verrà mostrata una lista di nomi (i siti web o le applicazioni a cui l'utente è registrato con username e password). L'utente scorrerà la lista dall'alto verso il basso premendo "A" o "B" dal tastierino numerico e potrà scegliere quali credenziali di un App inviare premendo il tasto "C".
Successivamente, l'utente si potrà autenticare inserendo un codice pin: se il pin inserito è corretto l'utente potrà proseguire con l'invio delle credenziali, altrimenti sarà invitato ad inserirlo nuovamente. Dopo l'autenticazione, le credenziali (username e password) saranno inviate decifrate al dispositivo collegato a PassChain premendo i tasti "A" e "B".
Dopo che le credenziali sono state inviate, il sistema automaticamente mostrerà la lista di nomi e, per accedere alle credenziali, l'utente dovrà nuovamente verificarsi tramite l'inserimento del codice pin.
PassChain potrà collegarsi all'app Desktop premendo il tasto "*" quando l'utente si troverà nella lista dei nomi delle applicazioni: in quel momento verrà instaurata la connessione e sia la scheda che l'app desktop potranno iniziare a comunicare.

2.1 Requisiti funzionali

Identificativo	Priorità	Descrizione
RF[1]	5	Il sistema deve autenticare l'utente, tramite il tastierino numerico ogni volta che richiede l'invio delle credenziali.
RF[2]	5	L'utente può modificare il codice pin tramite applicazione desktop.
RF[3]	5	Il sistema deve inviare i dati ad un dispositivo tramite il bluetooth.
RF[4]	5	Il sistema deve memorizzare un insieme di credenziali cifrate.
RF[5]	5	Il sistema deve potersi collegare all'applicazione desktop tramite protocollo MQTT.
RF[6]	5	Il sistema deve poter permettere di modificare, rimuovere ed aggiungere le credenziali scelte dall'utente tramite applicazione desktop.
RF[7]	4	Il sistema deve poter trasmettere dei suoni quando l'utente pigia sui tasti del tastierino numerico.

2.2 Requisiti non funzionali

Identificativo	Priorità	Descrizione
RNF[1]	5	Il sistema deve garantire la sicurezza delle credenziali memorizzate.
RNF[2]	5	Il sistema deve collegarsi ad un dispositivo e inviare le credenziali entro pochi secondi.

3. Strumenti Software e Hardware utilizzati

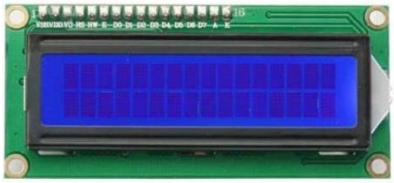
3.1 Dispositivi hardware

Il sistema dovrà essere composto dai seguenti componenti hardware:

- **Scheda ESP32**, per la gestione del sistema, dei sensori esterni e dell'interfacciamento con i dispositivi su cui sarà necessario inserire le credenziali di accesso (Computer, Smartphone ecc…).

- **Tastierino numerico**, attraverso il quale l'utente può navigare all'interno del sistema premendo dei pulsanti appositi.

- **Display LCD**, permette la visualizzazione a schermo delle istruzioni che l'utente deve seguire.



- **Buzzer**, emette un suono all'accensione e ogni qual volta che l'utente pigia sul tastierino numerico.

3.2 Micropython

La scheda ESP32 è stata programmata utilizzando come linguaggio di programmazione **micropython**. L'IDE di supporto per la programmazione della board è stato "Thonny" il quale ha permesso la scrittura del codice python e il suo caricamento sulla scheda.

Tra le librerie utilizzate e modificate per il sistema abbiamo:

- Bluetooth: **HID_services** (**LINK**)
- Protocollo MQTT: **umqttsimple** (**LINK**)
- Tastierino numerico: **keypad** (**LINK**)
- Buzzer: **buzzer_music** (**LINK**)

Per quanto riguarda il funzionamento del display è stata scritto un driver apposito.

3.3 GUI

L'interfaccia grafica è un'applicazione desktop che permette all'utente di effettuare il setup del dispositivo IoT, in particolare, l'utente può:

1. aggiungere nuove credenziali;
2. eliminare le credenziali;
3. modificare le credenziali già esistenti;
4. modificare il codice pin.

Per accedere all'applicazione, l'utente dovrà inserire lo stesso codice pin utilizzato per il dispositivo IoT. La GUI è realizzata interamente in Java (sia back-end che front-end), in particolare per il front-end sono state utilizzate come tecnologie JavaFX e CSS.

3.4 Mock-up

Di seguito sono mostrati dei mock-up di alcune funzionalità dell'interfaccia grafica.

Fig. 1 - Autenticazione

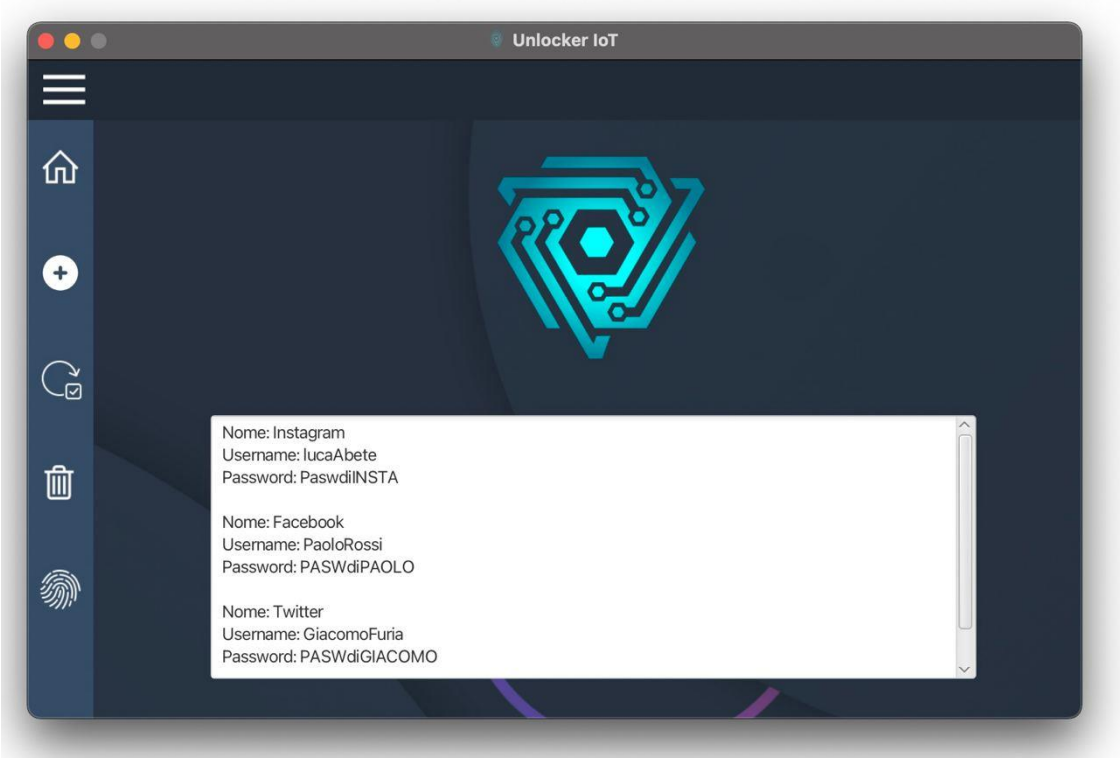


Fig. 3 - Dashboard

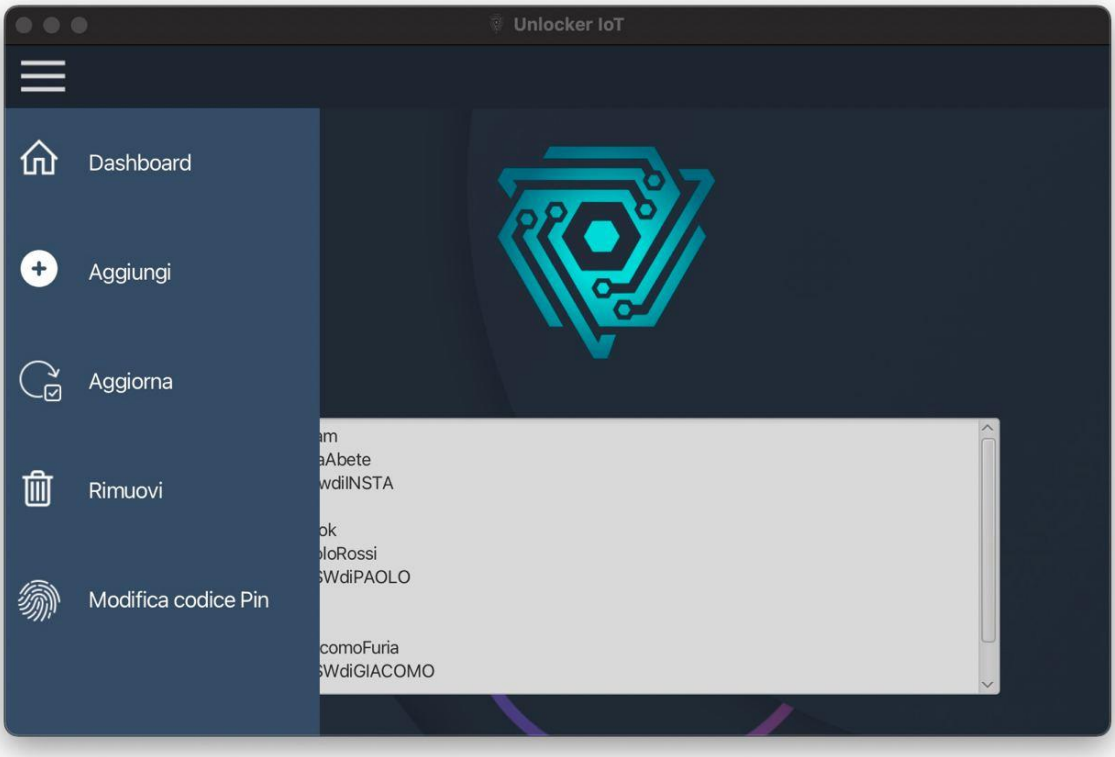


Fig. 4 - Dashboard (con side menu)

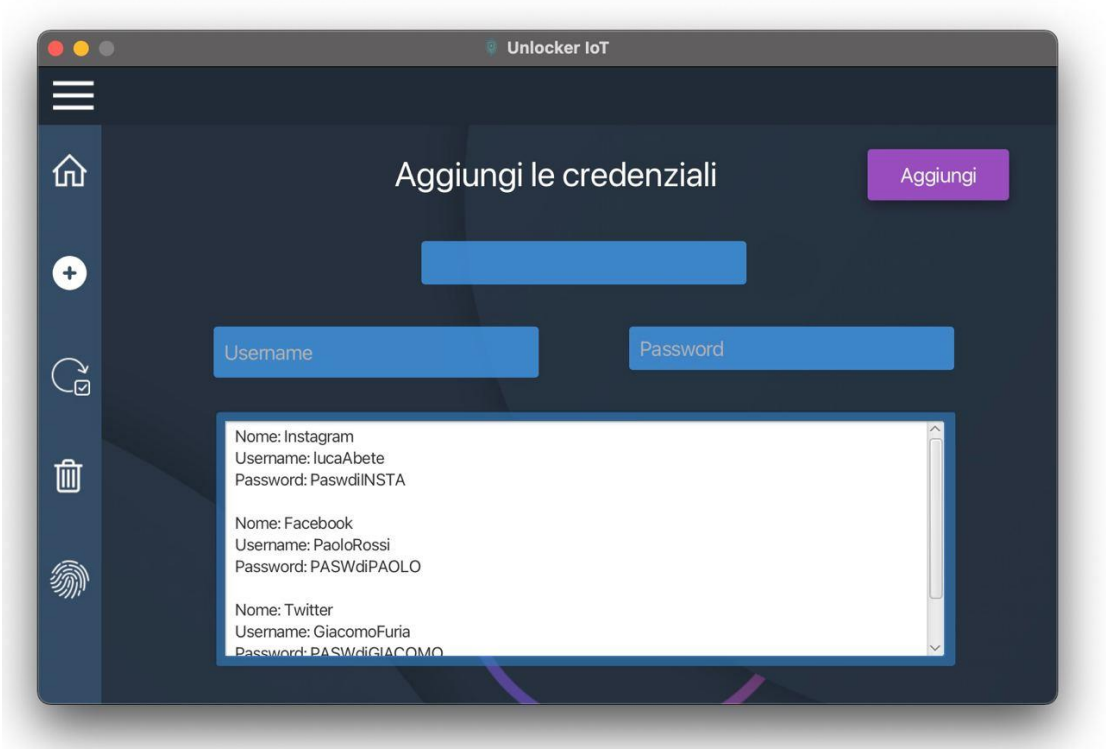


Fig. 5 - Aggiungi credenziali

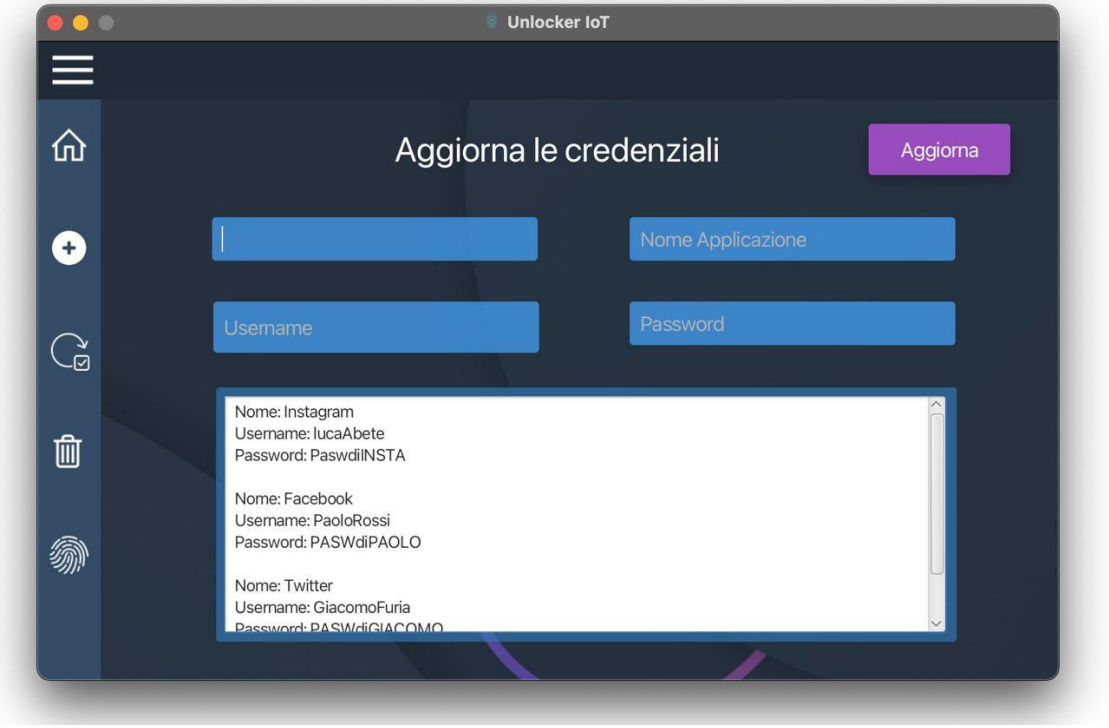


Fig. 6 - Modifica credenziali

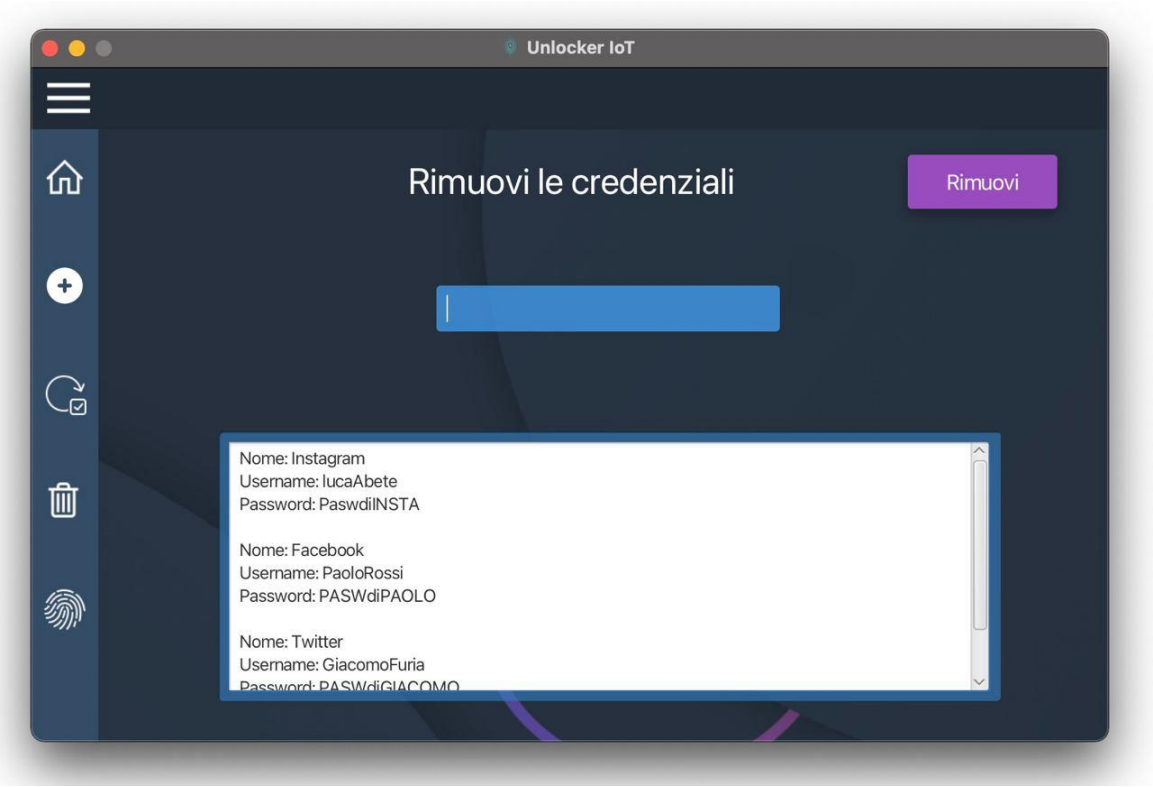


Fig. 7 - Rimuovi credenziali

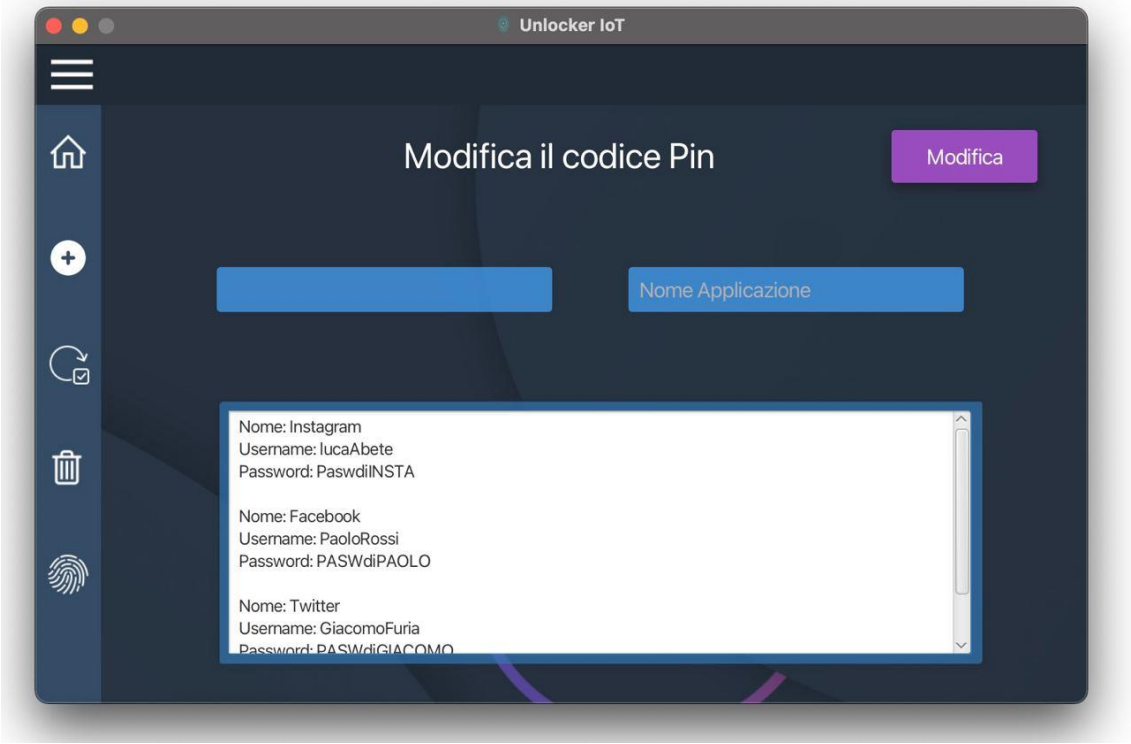


Fig. 8 - Modifica il codice Pin