UNIVERSITÀ DEGLI STUDI DI SALERNO

Corso di Laurea Magistrale in Informatica, prof. ssa Rita Francese

a.a 2024/2025

ENTERPRISE MOBILE APPLICATION DEVELOPMENT

MockUp

Studenti:

Marta Coiro matr. 0522501611

Katia Buonocore matr 0522501744

Gabriele Coralluzzo matr 0522501784

Umberto Della Monica 0522501617

Coach Aziendale:

Gabriele Ciliberti

LinearIT

INDICE

1. Introduzione

1.1. Descrizione del progetto

Con la crescente diffusione di dispositivi smart e sistemi IoT nelle case, dalle telecamere di sicurezza agli elettrodomestici intelligenti, le reti domestiche stanno diventando sempre più vulnerabili agli attacchi informatici. Ogni dispositivo connesso rappresenta un potenziale punto di accesso per minacce esterne, che possono compromettere la privacy e la sicurezza dell'intera rete domestica. Sebbene molti utenti non siano consapevoli di questi rischi, le violazioni della sicurezza nei contesti domestici sono in costante aumento e includono attacchi come l'accesso non autorizzato, il furto di dati, e l'intercettazione del traffico di rete.
In questo contesto, il nostro progetto mira a sviluppare un dispositivo hardware di sicurezza dedicato alla rete domestica che si posiziona come punto di controllo e protezione per tutti i dispositivi connessi. Tale dispositivo funzionerà sia come IDS (Intrusion Detection System) che come IPS (Intrusion Prevention System), rilevando e prevenendo attività sospette o pericolose nel traffico di rete, con una particolare attenzione alla protezione contro minacce esterne e all'intercettazione di comportamenti anomali.
Il dispositivo sarà supportato da un'applicazione mobile intuitiva, che servirà come interfaccia per il monitoraggio e la gestione delle impostazioni di sicurezza. L'applicazione notificherà in tempo reale qualsiasi evento di sicurezza e permetterà agli utenti di avere un controllo completo e personalizzabile del loro ambiente di rete, anche senza particolari competenze in ambito cybersecurity.

1.2. Obiettivi del progetto

1. **Obiettivo Primario**

Il principale obiettivo del progetto è fornire agli utenti domestici uno strumento semplice ed efficace per:

- **Monitorare in tempo reale** il traffico di rete e la sicurezza dei dispositivi connessi.
- **Rilevare e prevenire potenziali minacce** attraverso un sistema di sicurezza automatizzato basato su Suricata, una piattaforma open-source per l'analisi del traffico di rete.
- **Fornire uno storico degli eventi** per consentire analisi retroattive dei comportamenti di rete, monitorare potenziali trend di sicurezza e ottimizzare la configurazione dei dispositivi.

2. **Obiettivi Specifici**
   - **Analisi e Rilevamento delle Minacce**: Grazie all'utilizzo di un IDS/IPS, il dispositivo è in grado di monitorare continuamente il traffico di rete e segnalare eventuali comportamenti anomali. Suricata, configurato per operare sia in modalità IDS che IPS, consente di rilevare minacce come accessi non autorizzati, tentativi di phishing, malware, e altre attività sospette.
   - **Archiviazione dei Dati in Cloud**: Gli eventi rilevati saranno memorizzati in un'infrastruttura cloud per garantire la disponibilità di uno storico completo, che consente l'analisi dettagliata degli incidenti di sicurezza. Questo approccio supporta anche l'aggiunta di funzionalità predittive in futuro, come il riconoscimento di pattern di comportamento anomalo basati su dati storici.

- **Personalizzazione della Sicurezza**: Attraverso l'app mobile, l'utente può configurare facilmente le impostazioni di sicurezza.
- **Estensibilità per Future Funzionalità**: La piattaforma è pensata per essere estendibile, in modo da poter implementare rapidamente nuove funzioni di sicurezza, come un ad-blocker per la protezione della privacy o un controllo parentale per i contenuti destinati ai più piccoli.
- **Responsive design**: Adottare un **responsive design** per garantire che l'applicazione sia accessibile e utilizzabile su una varietà di dispositivi e dimensioni di schermo.

1.3. Obiettivi dei mockup

I mockup dell'applicazione mobile mirano a definire in dettaglio l'interfaccia e l'esperienza utente che consentiranno la gestione e il monitoraggio del dispositivo di sicurezza per la rete domestica. In questa fase del progetto, è essenziale visualizzare in modo chiaro la navigazione, i flussi utente, e le principali funzionalità dell'app, in modo che gli sviluppatori e le parti interessate possano avere un quadro completo di come il prodotto finale interagirà con gli utenti.
Gli obiettivi principali del mockup sono suddivisi come segue:

Progettare un'Interfaccia Utente (UI) Intuitiva e Accessibile: Creare un'interfaccia semplice e chiara che consenta anche agli utenti meno esperti di comprendere lo stato della loro rete domestica e intervenire rapidamente in caso di minacce alla sicurezza.

Definire l'Estetica e il Tone of Voice della Comunicazione: Creare un design visivo che ispiri fiducia e trasmetta un senso di sicurezza e protezione all'utente.

Questi obiettivi per i mockup garantiscono una rappresentazione completa delle funzionalità dell'applicazione mobile e del percorso dell'utente, agevolando il lavoro di sviluppo e di revisione del progetto, con una visione chiara delle necessità di design e di usabilità.

1.4. Target del Progetto

Il target principale di questo progetto è costituito dagli utenti domestici e dalle piccole aziende che utilizzano dispositivi smart e sistemi IoT, ma che non dispongono di strumenti avanzati per la protezione e il monitoraggio della rete. Nello specifico, il progetto è rivolto a tre principali gruppi di utenti, con esigenze e livelli di conoscenza della sicurezza informatica variabili:

1. **Famiglie e Utenti Domestici**

Questo segmento include famiglie e singoli utenti che possiedono più dispositivi smart come smartphone, tablet, elettrodomestici intelligenti, videocamere di sorveglianza e altri sistemi IoT. Questi utenti:

- **Esigenze**: Richiedono protezione per tutti i dispositivi della casa, soprattutto per garantire la privacy della famiglia e dei bambini.
- **Livello di Competenza Tecnologica**: Solitamente di livello medio-basso, senza conoscenze avanzate di sicurezza informatica.

- **Benefici Principali**: Questo progetto fornirà a questi utenti una protezione della rete domestica facile da gestire, permettendo loro di monitorare le minacce e bloccare attività sospette senza doversi addentrare in configurazioni complesse.

2. Piccole Aziende e Professionisti

Piccole aziende e professionisti che lavorano da casa rappresentano un target secondario importante per questo dispositivo. In questi contesti, la sicurezza dei dati e la protezione della rete sono fondamentali, soprattutto per la gestione di informazioni sensibili come dati di clienti e comunicazioni aziendali.

- **Esigenze**: Necessitano di protezione avanzata per le reti domestiche e per i dispositivi di lavoro, con la possibilità di monitorare attività sospette e impedire accessi non autorizzati.
- **Livello di Competenza Tecnologica**: Generalmente di livello medio, con una conoscenza base della sicurezza informatica.
- **Benefici Principali**: L'utilizzo di questo dispositivo permette ai professionisti di avere un sistema di sicurezza completo e automatizzato per ridurre il rischio di attacchi mirati, con una gestione facile e centralizzata tramite app mobile.

3. Appassionati di Tecnologia e di Smart Home

Gli utenti tech-savvy, che già utilizzano numerosi dispositivi smart in casa e sono interessati a gestire e proteggere ogni aspetto della propria rete, sono un target ideale per le funzionalità avanzate di questo progetto.

- **Esigenze**: Cercano soluzioni per il monitoraggio approfondito della rete e la personalizzazione delle impostazioni di sicurezza, con opzioni per il controllo dettagliato dei singoli dispositivi.
- **Livello di Competenza Tecnologica**: Elevato, con un interesse particolare verso le tecnologie di sicurezza e di automazione domestica.
- **Benefici Principali**: Il dispositivo offre loro un controllo avanzato sul traffico di rete, permettendo di analizzare e ottimizzare la sicurezza della propria smart home, con la possibilità di configurare funzionalità aggiuntive come blocco degli annunci e controllo parentale.

4. Caratteristiche Comuni del Target

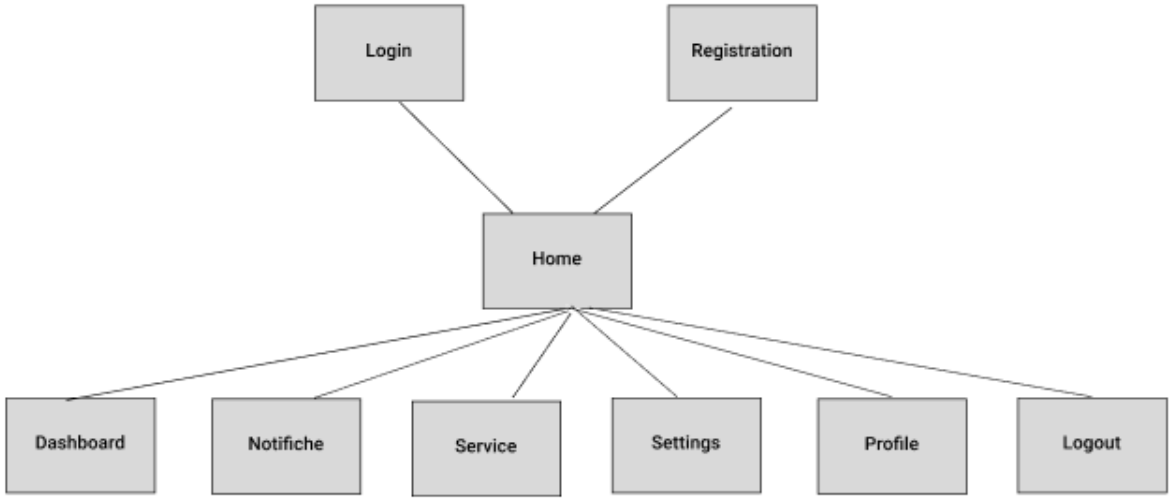
Tutti i gruppi di target condividono alcune caratteristiche e necessità di base:

- **Sicurezza e Privacy**: Protezione contro le minacce informatiche che possano compromettere la sicurezza dei dati e della privacy.
- **Semplicità d'Uso**: Desiderio di soluzioni intuitive che non richiedano competenze tecniche avanzate per essere gestite.
- **Affidabilità**: Preferiscono soluzioni che possano funzionare in background, senza compromettere la connettività e le prestazioni della rete.
- **Flessibilità e Scalabilità**: Necessitano di una piattaforma che possa adattarsi alle esigenze attuali ma anche ampliarsi nel tempo, con la possibilità di aggiungere nuove funzionalità di sicurezza e controllo.

Il target di questo progetto comprende quindi un’ampia gamma di utenti, dai meno esperti ai più tecnicamente preparati, con un’esigenza comune: proteggere la propria rete domestica e i dispositivi connessi da minacce crescenti, in modo semplice, affidabile e personalizzabile.

2. Struttura dei mockup

2.1. Flusso di navigazione



Home Page dell'Applicazione
La Home Page dell'applicazione è progettata per fornire un accesso rapido e intuitivo a tutte le funzionalità principali, ottimizzando l'esperienza utente. La struttura è suddivisa in diverse sezioni, ognuna con un focus specifico.

1. **Intestazione**
   Pulsante di Logout: Situato in alto a destra, consente agli utenti di disconnettersi facilmente dall'applicazione. Al tocco, appare un messaggio di conferma per garantire che l'utente desideri davvero effettuare il logout.
   Icona delle Notifiche: Accanto al pulsante di logout, l'icona delle notifiche (un campanello o una bolla di messaggio) mostra un badge con il numero di notifiche non lette.
   Al tocco, si apre un elenco a discesa con le notifiche recenti e un pulsante per visualizzare tutte le notifiche.
2. **Sezione Dashboard (icona Dashboard)**
   Tale icona mi permette di arrivare alla pagina delle varie statistiche del mio router
   Grafico Statistiche Mensili: Visualizza un grafico interattivo che mostra l'uso dei dati mensile, evidenziando i picchi e i periodi di inattività. Include anche un riepilogo delle statistiche di utilizzo, come il totale dei dati utilizzati e la media giornaliera.

3. **Sezione Servizi (Icona Servizi)**
   Tale icona permette di arrivare alla pagina dei “Servizi”. Attivazione delle Regole di Suricata.io: Un'interfaccia che consente di attivare o disattivare specifiche regole di sicurezza. Ogni regola è accompagnata da una breve descrizione, con toggle per l'attivazione/disattivazione.
4. **Sezione WiFi Settings (icona Wifi)**
   Informazioni sul Raspberry Pi: Mostra dettagli come l'indirizzo IP locale, il nome della rete (SSID) e lo stato della connessione. Modifica della Password del WiFi: Un modulo per inserire e confermare una nuova password per la rete WiFi, con feedback sul successo o errore dell'operazione.
5. **Sezione Profilo (icona User)**
   Credenziali Utente: Visualizza il nome utente e l'email dell'account, con opzioni per modificare la password e per cancellare l'account. Include pulsanti per salvare le modifiche e gestire le credenziali in modo sicuro.
6. **Sezione Notifiche (icona dell’intestazione)**
   Visualizzazione delle Notifiche: Elenco delle notifiche recenti ricevute dal Raspberry Pi, in ordine cronologico. Ogni notifica include dettagli come il tipo di evento, data e ora, e informazioni specifiche sull'evento. Include anche un'opzione per filtrare o cercare tra le notifiche.

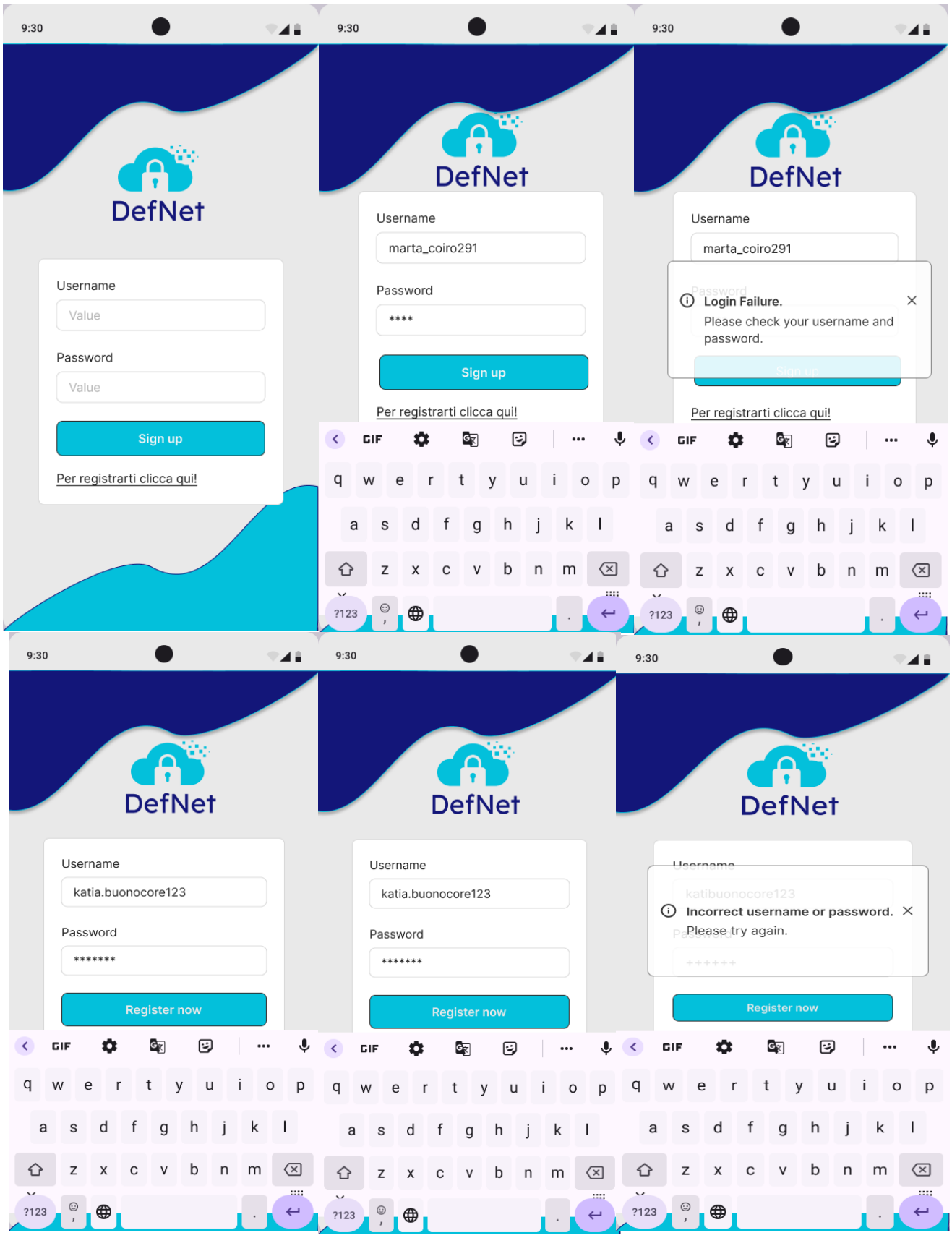
3. Dettagli delle schermate

3.1. Versione mobile

Di seguito possiamo visualizzare in dettaglio la rappresentazione dei mockup per la versione mobile della nostra applicazione.

Perché “DefNet”?

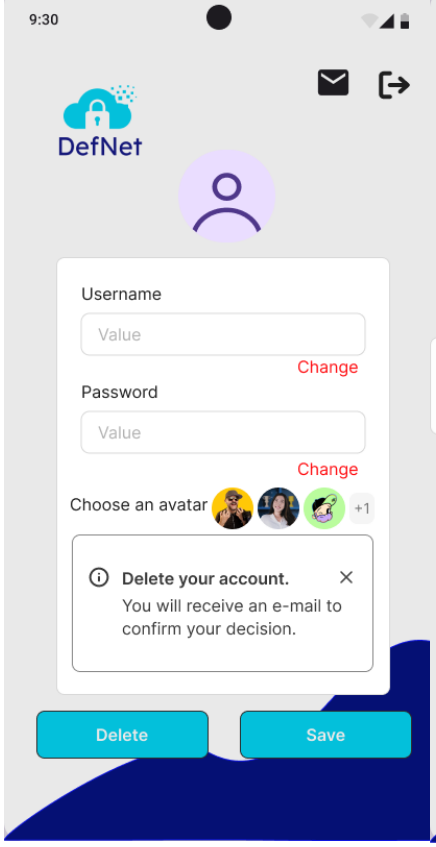
Questo nome è dato dall’unione di due termini “Defender” “Network”, per rendere maggiormente l’idea di proteggere la nostra rete.

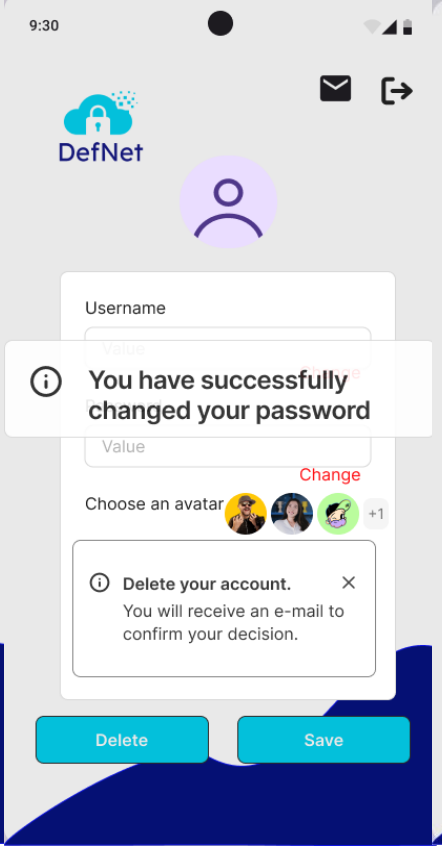

9:30
DefNet
Username
Value
Password
Value
Sign up
Per registrarti clicca qui!
9:30
DefNet
Username
marta_coiro291
Password
****
Sign up
Per registrarti clicca qui!
9:30
DefNet
Username
marta_coiro291
Login Failure.
Please check your username and password.
Sign up
Per registrarti clicca qui!
9:30
DefNet
Username
katia.buonocore123
Password
****
Register now
9:30
DefNet
Username
katia.buonocore123
Password
****
Register now
9:30
DefNet
Incorrect username or password.
Please try again.
Register now

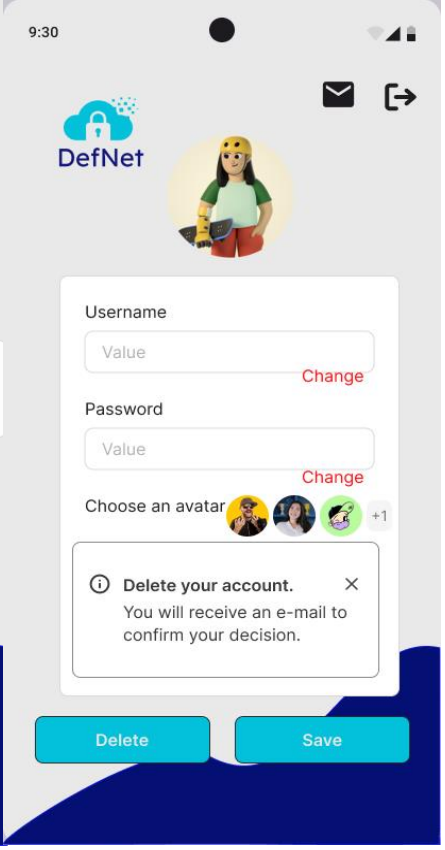

9:30
DefNet
Hello!
Marta Coiro
Statistics
Service
Profile
Wi-Fi Settings

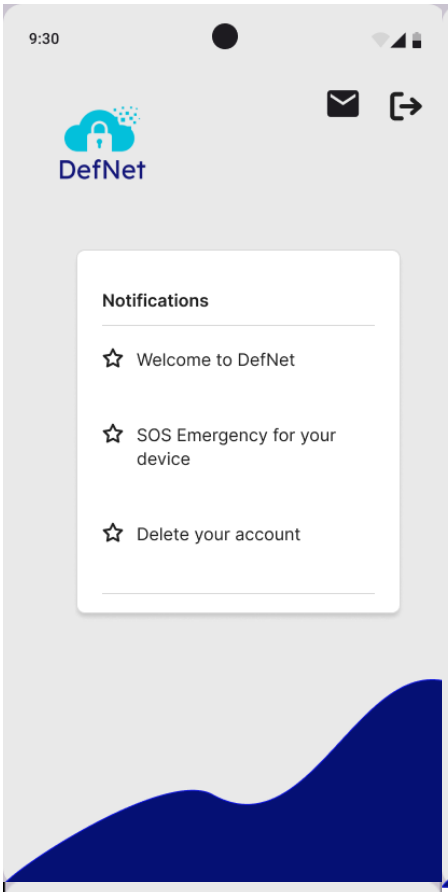
9:30
DefNet
Statistics
Mb
I _ Days _ I
Device Management
LAPTOP-1JN17EKK
IP: 192.168.1.161
Mac: d8:f3:bc:6c:5d:e3
Band: Wi-Fi 5GHz

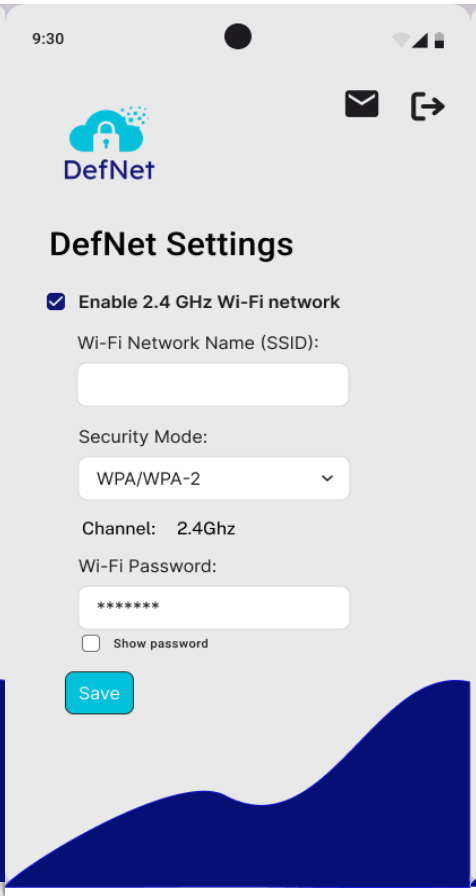
9:30
DefNet
Services
Enable No ADS
Threat control
Ad-Blocking

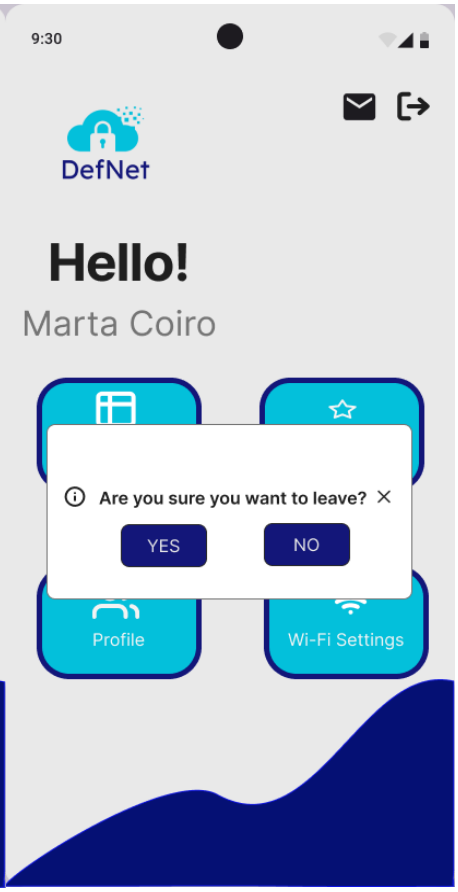

9:30
DefNet
Username
Value
Change
Password
Value
Change
Choose an avatar
+1
Delete your account.
You will receive an e-mail to confirm your decision.
Delete
Save


9:30
DefNet
Username
Value
Change
You have successfully changed your password
Password
Value
Change
Choose an avatar
+1
Delete your account.
You will receive an e-mail to confirm your decision.
Delete
Save

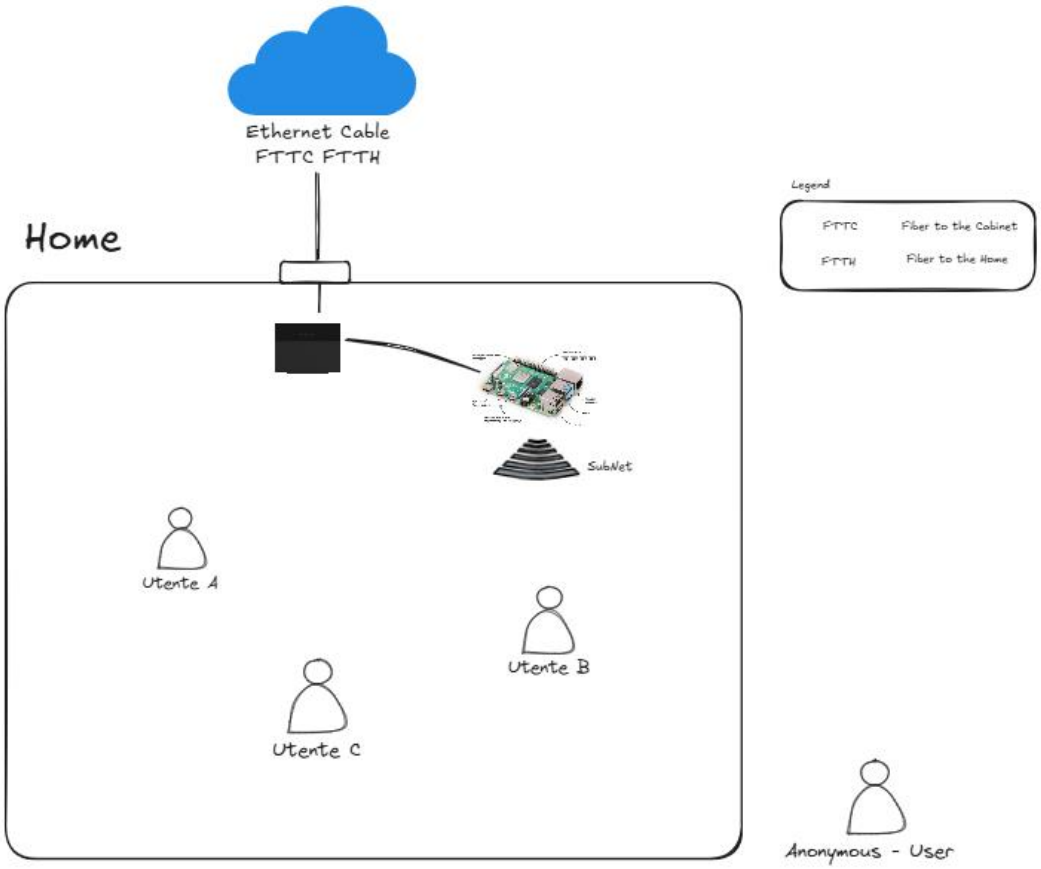

9:30
DefNet
Username
Value
Change
Password
Value
Change
Choose an avatar
+1
Delete your account.
You will receive an e-mail to confirm your decision.
Delete
Save

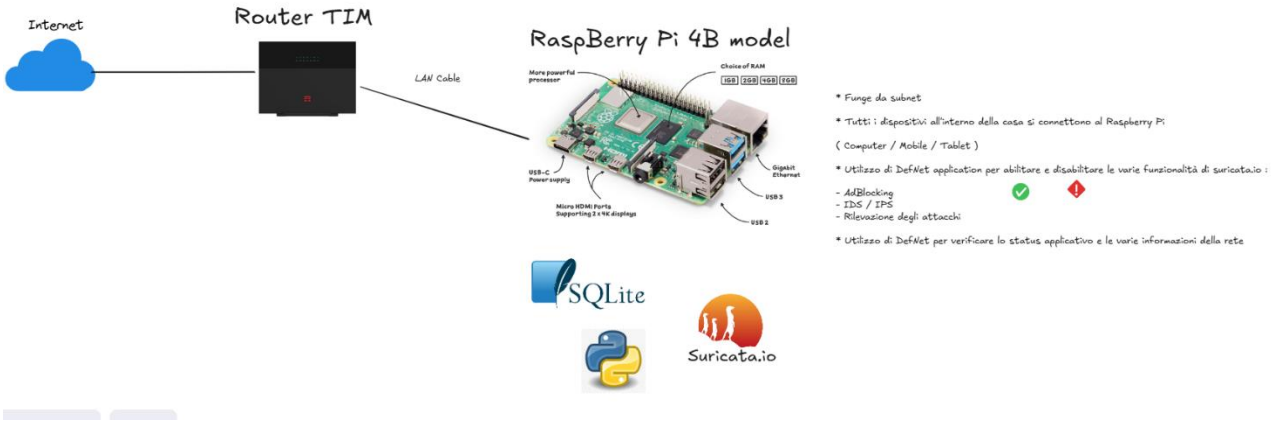

9:30
DefNet
Notifications
Welcome to DefNet
SOS Emergency for your device
Delete your account


9:30
DefNet
DefNet Settings
Enable 2.4 GHz Wi-Fi network
Wi-Fi Network Name (SSID):
Security Mode:
WPA/WPA-2
Channel: 2.4Ghz
Wi-Fi Password:
****
Show password
Save


9:30
DefNet
Hello!
Marta Coiro
Are you sure you want to leave?
YES
NO
Profile
Wi-Fi Settings


9:30
DefNet


Ethernet Cable
FTTC FTTH
Legend
FTTC
Fiber to the Cabinet
FTTH
Fiber to the Home
Home
SubNet
Utente A
Utente B
Utente C
Anonymous - User


Internet
Router TIM
LAN Cable
RaspBerry Pi 4B model
* Funge da subnet
* Tutti i dispositivi all'interno della casa si connettono al Raspberry Pi
(Computer / Mobile / Tablet)
* Utilizzo di DefNet application per abilitare e disabilitare le varie funzionalità di suricata.io :
- AdBlocking
- IDS / IPS
- Rilevazione degli attacchi
* Utilizzo di DefNet per verificare lo status applicativo e le varie informazioni della rete
SQLite
Suricata.io

4. Palette colori