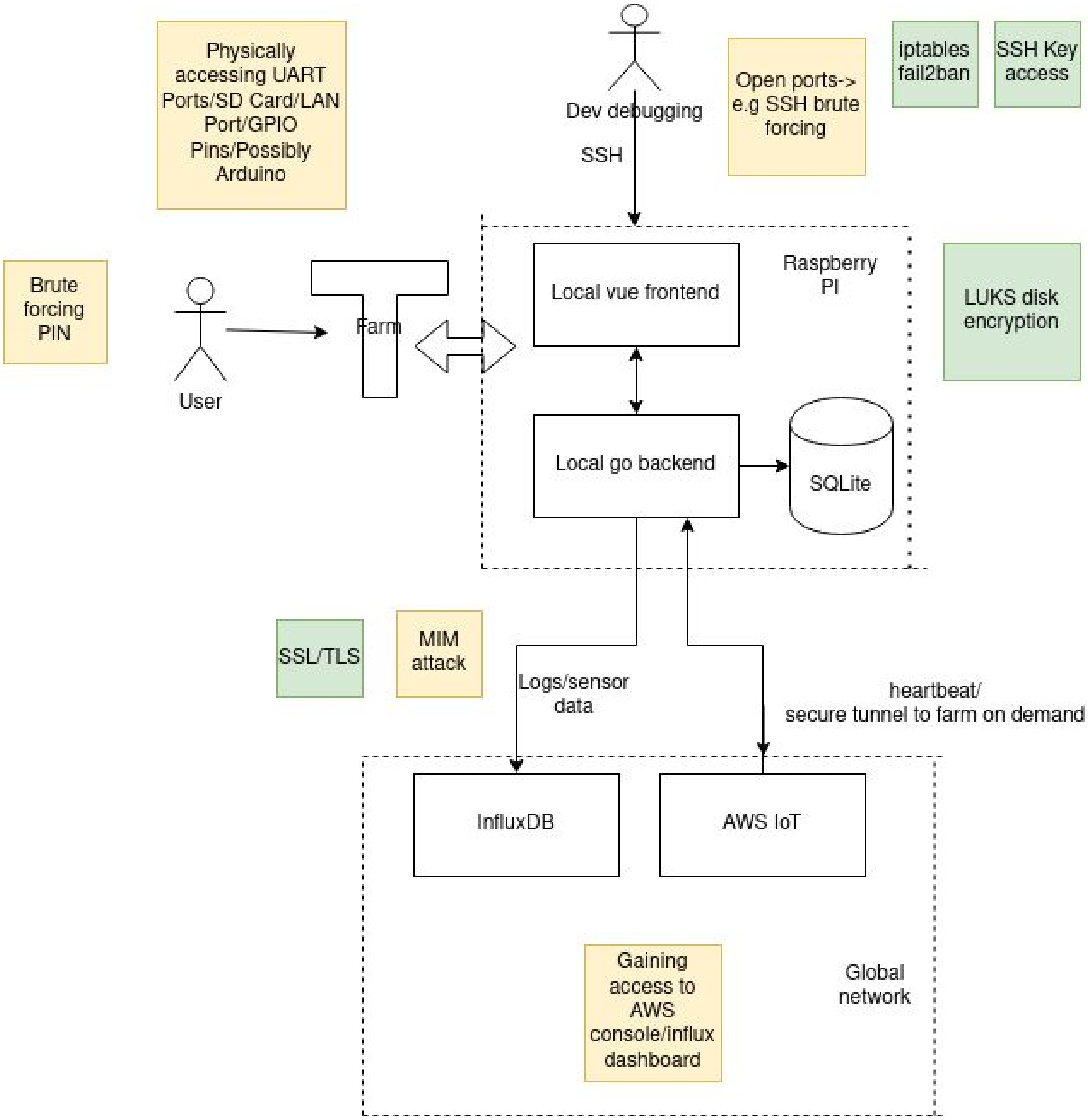
Security Documentation

Project: Susteyn
Status: 20.11.2020

Threat model:



Threats:

On the Thing level: (The farm itself)

-Physically stealing the raspberry/SD Card and gaining access to data including tokens
-Accessing USB Ports/LAN Ports/GPIO’s/Arduino
-Brute-forcing 4 digit PIN on interface to access settings like Wifi AP

On the Local network level: (The semi-public Wifi the farm will be usually connected to)

-Man in the middle attacks like:
 -DNS and ARP spoofing
 -Rogue AP by simply switching the wifi the farm is connected to
 -SSL stripping
-SSH brute forcing

On the Global Network level:

-Impersonating a farm
-Gaining access to docker hub and modifying images
-Gaining access to github repository

On the cloud level:

-Gaining access to AWS Console and therefore each and every farm

List of measures implemented/planned:

On the Thing level: (The farm itself)

-Changing all default users and passwords
-Physically securing the raspberry with a case/lock/zymkey
-Blocking/desolder unused Ports
-Allowing only known USB devices to connect
-LUKS encryption of SD card. Keyfile stored on separate USB stick that is needed to boot
-Anti-tamper with USB stick that needs to be removed when accessing raspberry
-USB Access key is needed to modify settings
-Regular security audits using Lynis

On the Local network level: (The semi-public Wifi the farm will be usually connected to)

-HTTPS is forced
-Wifi settings are protected by USB key
-SSH using keys instead of password, possibly 2fa
-Fail2ban prevents multiple wrong login attempts
-Possibly VPN

On the Global Network level:
-Every farm has a unique token and device certificates to AWS and Influx.
-Signing docker images
-Influx/AWS monitoring farm values and sending alerts whenever an anomaly occurs

On the cloud level:
-Strong passwords
-Hope that AWS does not suffer from breach