Device Management & Security for IoT Platform

By Kashish Kitawat, Pallawi Kumari, Pavani Sapparapu, Shamman Noor Shoudha

Purpose

- To Encrypt the raw data, read from the sensors using AES-128
- To Decrypt the data and providing the filtered data according to the Role (Role-Bases Access Control)
- Using Key Management we can have different users with different passwords

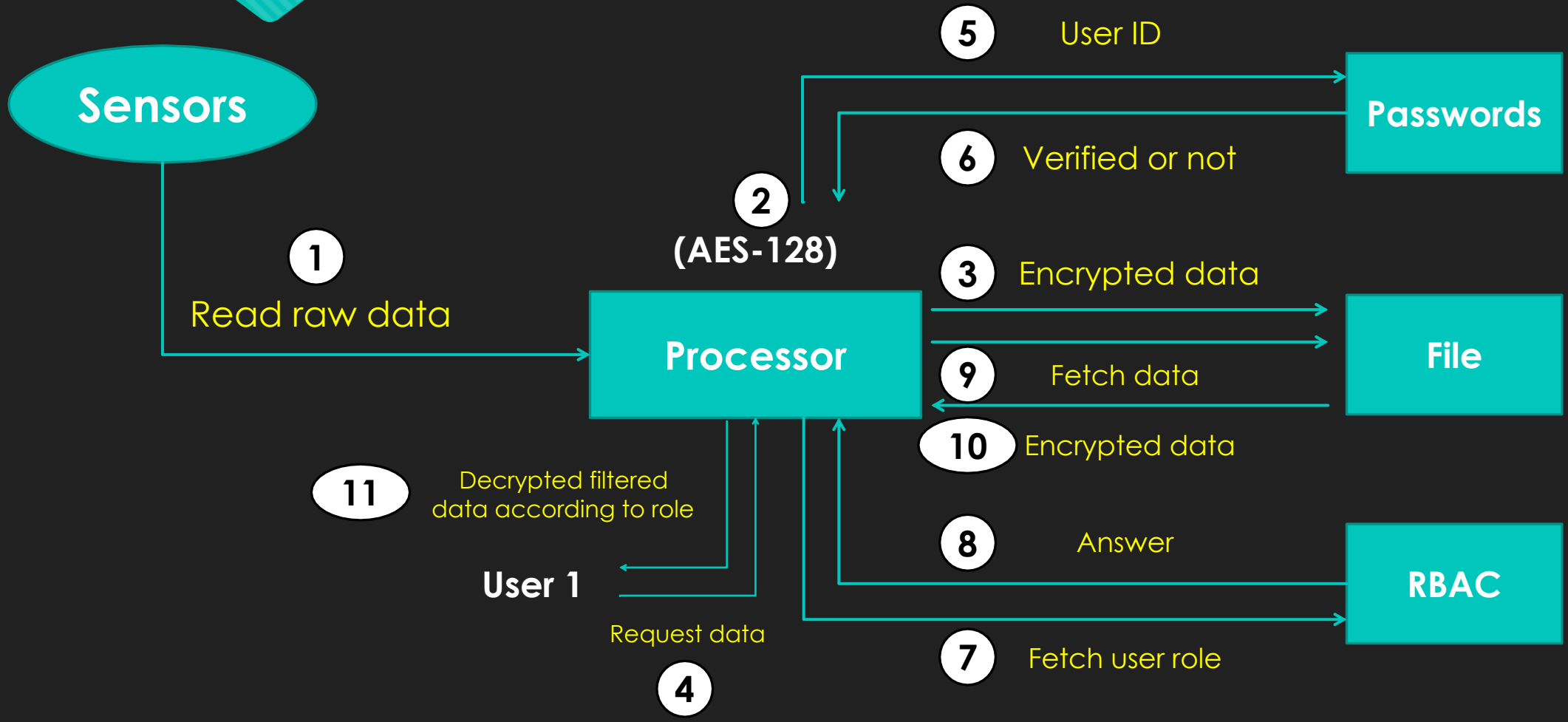
Specification

- Processor:
  - Encrypts the data using the AES-128 algorithm.
  - Stores and fetches the data from the storage file/cloud
  - Verifies the identity of the user
  - Filters the data according the user's access
- Files: All the files will be in an encrypted form
  - Storage File: Stores the encrypted data
  - RBAC File: Stores the roles of the users
  - Password File: Stores the passwords of the users.

Objective

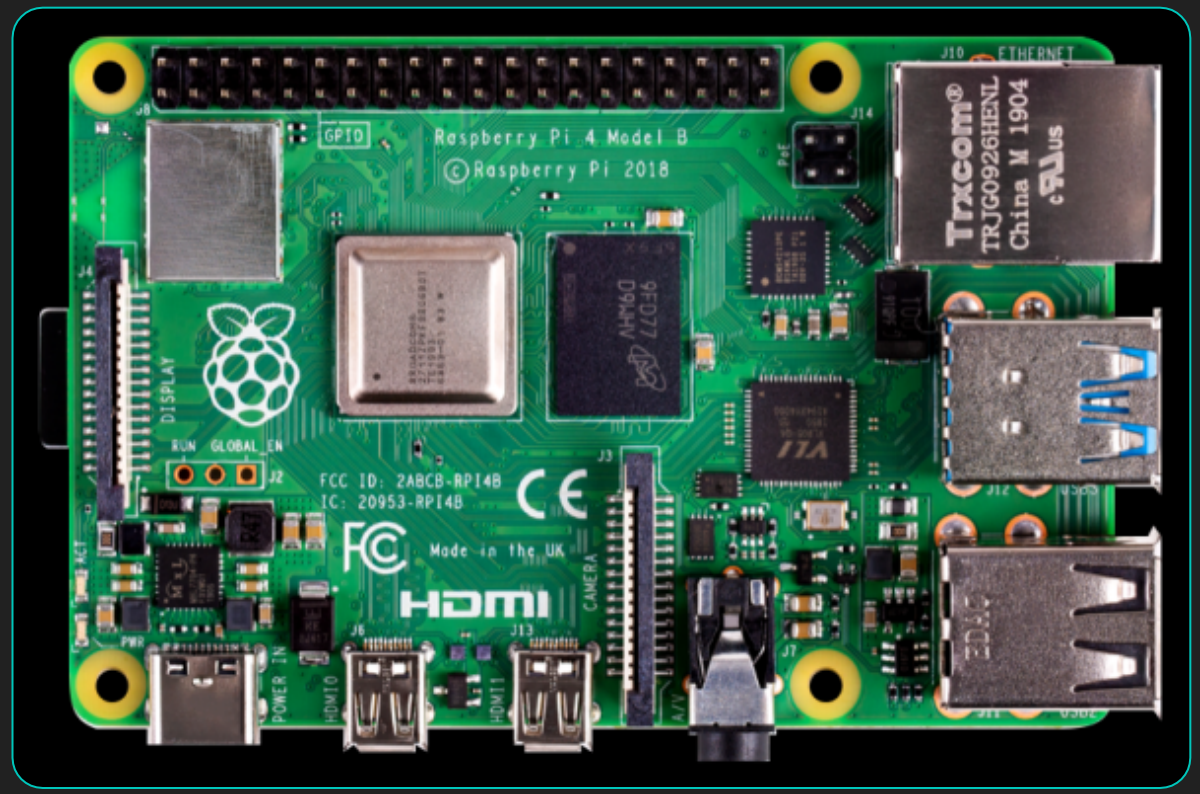
- To verify the user's identity
- To verify if the user has access to view/request that data

Flow diagram



Hardware component

- Raspberry Pi
  - Processor speed 1.5GHz with Quad core ARM Processor
  - For AES-128, we require 1.25GHz single core processor. So we can have 4 individual processes running simultaneously.



Software Tools

- Python3
  - Pre-defined libraries which helps in doing AES encryption
  - Less dependencies
- Linux
  - Light-weight
  - Inbuilt commands

Timeline

Days	Work
2/24 – 3/12	Implementation and Procuring the hardware
3/12 – 3/26	Simulation
3/26 – 4/2	Hardware Implementation
4/2 – 4/16	Verifying the results on the hardware (TESTING)