IoT Lab 3: OTA Firmware Update

Overview

This lab focuses on implementing an Over-the-Air (OTA) firmware update mechanism for IoT devices, for example: a temperature and humidity monitoring system. The goal is to enable remote firmware updates without physical access to the hardware, ensuring easy maintenance and feature upgrades.

Requirements

Design and implement an OTA update system for an IoT device based on Core-IoT platform.

Hardware:

- ESP32 or ESP32 S3 Development board.
- DHT20 or DHT11 temperature and humidity sensors.
- Connectors.

Technical Risks:

Test Plan

Test Cases:

- Firmware Upload Test: Upload a new firmware version to the server and trigger an OTA update.
- Data Integrity Check: Verify that temperature and humidity data continue to be sent correctly after an update.

Approach

- Set up the ESP32 with basic firmware that reads sensor data and transmits it to an IoT dashboard.
- Implement an OTA update mechanism using either HTTP or MQTT.
- Upload a new firmware version and trigger the update remotely.

Questions

- What are some security measures you can implement to prevent unauthorized OTA updates?
- How does your OTA update mechanism handle network interruptions?
- What methods can be used to verify the integrity of the new firmware before applying it?

Instructions:

- Initial Setup:
  - Run a "Hello World" example to verify that the ESP32 is functional.
  - Run a DHT20 example to ensure the sensor is working correctly.
- Implement OTA Update:
  - Configure the ESP32 to check for firmware updates over HTTP or MQTT.
  - Deploy an update server and host a new firmware version.
- Test the Update Process:
  - Trigger an OTA update and monitor the process.
  - Verify that the new firmware is running correctly after the update.
- Enhance Security (You only need to write down your solutions; no implementation is required).
  - Implement firmware signing and validation before installation.
  - Use authentication mechanisms to prevent unauthorized updates.

Resources