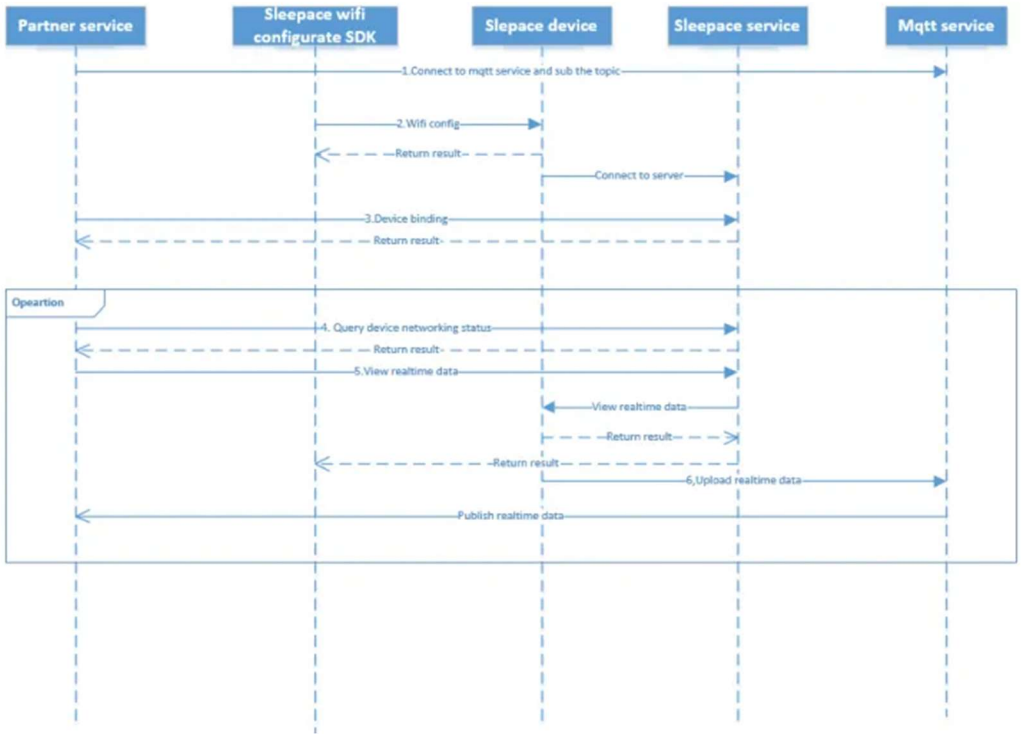
Scope Identification:

From an attacker's perspective, the scope of targeting an IoT sleep monitoring device includes exploiting communication vulnerabilities, breaching sensitive health data, disrupting service, and leveraging the device for broader network attacks. The focus would be on identifying weak points in the device's configuration, communication protocols, and physical security to gain unauthorized access or disrupt its intended operation

System Decomposition:

Sequence Diagram:



Protocols:

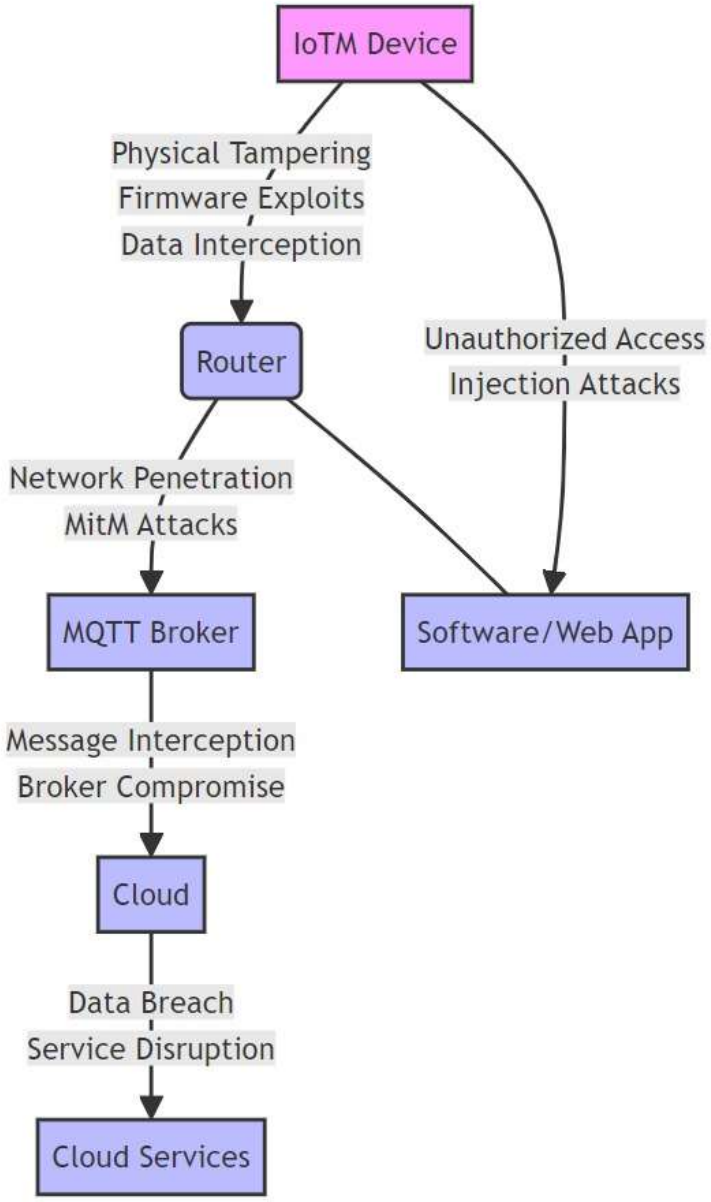
1) MQTT
2) WIFI

Device Environment:

1) Sleep monitoring Device
2) Router
3) MQTT broker
4) Software/Web APP
5) Cloud

Threat Identification:

Threat Vectors:



Possible Threat Events:

1. Man-in-the-Middle (MITM) Attacks

Description:

- In a MITM attack, an attacker intercepts communication between an MQTT client and broker. The attacker can eavesdrop, modify, or inject malicious messages into the communication stream.

Tools:

- **Wireshark**: Used to capture and analyze MQTT traffic. It can reveal unencrypted payloads, credentials, and other sensitive information.
- **MITMproxy**: A tool that can intercept, inspect, and modify MQTT traffic, especially useful when traffic is over HTTP or HTTPS.
- **Bettercap**: A powerful MITM framework that can intercept MQTT traffic and perform various attacks, such as credential theft or data manipulation.

2. Credential Brute-Forcing

Description:

- Attackers attempt to gain unauthorized access to the MQTT broker by brute-forcing credentials (username and password). If the broker is not properly secured, this can lead to full control over the MQTT communication.

Tools:

- **Hydra**: A parallelized login cracker that can be used to brute-force MQTT credentials.
- **Medusa**: Another parallel login brute-forcer that supports MQTT protocol.
- **Patator**: A flexible brute-forcing tool that can be used for MQTT credential attacks.

3. Denial of Service (DoS)

Description:

- In a DoS attack, the attacker floods the MQTT broker with a large number of connection requests, publish messages, or subscriptions, overwhelming the broker and causing it to crash or become unresponsive.

Tools:

- **MQTT-PWN**: A tool designed specifically to perform DoS attacks against MQTT brokers.
- **Slowloris**: Although not specific to MQTT, it can be adapted to perform slow DoS attacks against MQTT brokers by opening multiple connections slowly.
- **Hulk**: A DoS tool that can be configured to generate a large number of requests, overwhelming the MQTT broker.

4. Packet Injection

Description:

- Attackers inject malicious MQTT packets into the network, which can be used to disrupt communication, send false information, or control IoT devices.

Tools:

- **MQTTfx**: A client tool that can be used to publish and subscribe to topics, but also to inject packets manually to test the broker's response to malformed or unexpected packets.
- **MQTTShell**: A command-line tool that can be used to interact with MQTT brokers and clients, allowing for the injection of custom packets.
- **Scapy**: A powerful packet manipulation tool that can be scripted to create and send custom MQTT packets to a broker.

5. Replay Attacks

Description:

- In a replay attack, the attacker captures MQTT messages and retransmits them to the broker. This can cause devices to repeat actions or expose vulnerabilities in the broker's handling of duplicate messages.

Tools:

- **Wireshark**: Used to capture MQTT traffic, which can then be replayed.
- **Scapy**: Can be used to resend captured packets, facilitating replay attacks.
- **tcpreplay**: A suite of tools to replay captured network traffic, including MQTT messages.

6. Topic Hijacking

Description:

- Topic hijacking occurs when an attacker subscribes to a topic of interest and then publishes malicious data under the same topic. This can confuse or compromise the integrity of the data for legitimate subscribers.

Tools:

- **MQTT-Spy**: A Java-based tool that allows subscribing and publishing to MQTT topics, useful for testing hijacking scenarios.
- **Mosquitto_pub and Mosquitto_sub**: Command-line tools for subscribing and publishing to topics, allowing for testing of hijacking possibilities.
- **mqtt-cli**: Another command-line interface for interacting with MQTT brokers, enabling topic hijacking by subscribing and publishing to the same topics as legitimate clients.

7. Security Misconfiguration Exploitation

Description:

- MQTT brokers may be left with default or insecure configurations, such as no authentication, no encryption (using plain text communication), or open access to topics. Attackers can exploit these misconfigurations to gain unauthorized access or disrupt operations.

Tools:

- **MQTT Explorer**: A comprehensive MQTT client that allows exploration of all available topics, checking for misconfigurations or insecure access.
- **Nmap with NSE Scripts**: Nmap can be used to discover MQTT brokers and NSE scripts like `mqtt-subscribe` can be used to check for open topics and misconfigurations.
- **ZMQTT**: A tool for penetration testing MQTT setups, specifically designed to find security weaknesses and misconfigurations.

8. Message Spoofing

Description:

- An attacker can send forged messages under a legitimate topic, causing clients to act on false data. This could lead to actions like shutting down equipment, triggering alarms, or altering IoT device states.

Tools:

- **MQTT-PWN**: Aside from DoS attacks, it can also be used to spoof messages.
- **Scapy**: Can craft and send spoofed MQTT packets.
- **MQTTBox**: A versatile tool for testing and development that can simulate both clients and brokers, useful for spoofing scenarios.