**Secure Cellular Communication System for ESP32 with SIM7600**

**Overview**

This project implements a highly secure, cellular-based communication system for an ESP32 microcontroller using the SIM7600 modem. The focus is on MQTTS (MQTT over SSL/TLS) with AES-256 encryption to ensure secure data transmission.

**Key Features:**

* Secure MQTTS connection with certificate authentication
* AES-256 encryption for end-to-end message security
* LCD and LED for real-time feedback
* State machine and watchdog for system reliability
* Planned OTA updates for future firmware upgrades

**Implemented Features**

**Secure Communication with AES-256 Encryption**

* **Encryption and Decryption:**
  + Uses AES-256 CBC with PKCS7 padding
  + Encoded in Base64 for MQTT compatibility
* **Message Handling:**
  + Receives encrypted Base64 messages on server\_cmd, decrypts them, and sends plaintext to esp32\_status
  + Sends encrypted responses (e.g., "ESP32\_Denmark") in Base64 to esp32\_status

**MQTTS with Certificate Authentication**

* Uses the SIM7600's built-in MQTT stack for SSL/TLS-secured MQTTS communication
* **Certificate Authentication:** Uploads a custom SSL certificate to the SIM7600 for trusted connections
* **Multi-layer security:**
  + Username: "ESP32"
  + Password: "12345"
* **MQTT Topics:**
  + Subscribes to server\_cmd for incoming commands
  + Publishes responses to esp32\_status

**Hardware Integration**

* **LCD Display:** Shows decrypted messages (up to 16 characters)
* **LED Indicator:** Toggles for visual feedback when a message is received
* **SIM7600 Power Control:** Manages modem power via GPIO

**State Machine and Watchdog for Reliability**

* **State Machine:**
  + Handles modem initialization, network connection, and MQTTS setup
  + Uploads certificates and configures SSL settings dynamically
* **Watchdog Timer (30 seconds):**
  + Prevents system hangs by automatically restarting if necessary

**Debugging and Logging**

* **Extensive Serial Logging:**
  + Hex dumps and Base64 outputs for troubleshooting encryption, decryption, and MQTTS processes

**Future Enhancements (Planned)**

**OTA Firmware Updates (Not Yet Implemented)**

* Remote firmware updates via MQTTS
* Receives Base64-encoded firmware chunks on a dedicated topic (firmware/update)
* Writes updates to an OTA partition and reboots into the new firmware

**Key Advantages**

**Enhanced Security with MQTTS and AES-256**

* **Certificate Authentication:** Ensures only trusted devices can connect to the MQTT broker
* **SSL/TLS Encryption:** Protects against eavesdropping and tampering
* **Username and Password Authentication:** Adds another security layer
* **AES-256 Encryption:** Provides end-to-end message security

**Remote Management via Cellular Network**

* No Wi-Fi or Ethernet required, making it ideal for remote deployments
* Future OTA updates will allow remote firmware upgrades

**High Reliability**

* **State Machine:** Ensures robust modem control and connection handling
* **Watchdog Timer:** Prevents system lockups in the field

**Flexibility and Scalability**

* **Modular Design:** Easily extendable for new commands and features
* **LCD and LED Feedback:** Provides real-time status monitoring
* **Compatible with any MQTTS Broker** (e.g., EMQX Cloud)