CONEXIÓN SEGURA A SERVIDOR CON ESP8266 Y WI-FI PARA GARANTIZAR LA INTEGRIDAD Y SECRETO DE DATOS DE SENSORES

F. Marovic[(1)] y J. Jorge[(1)]

(1) Departamento de electrónica e informática centro

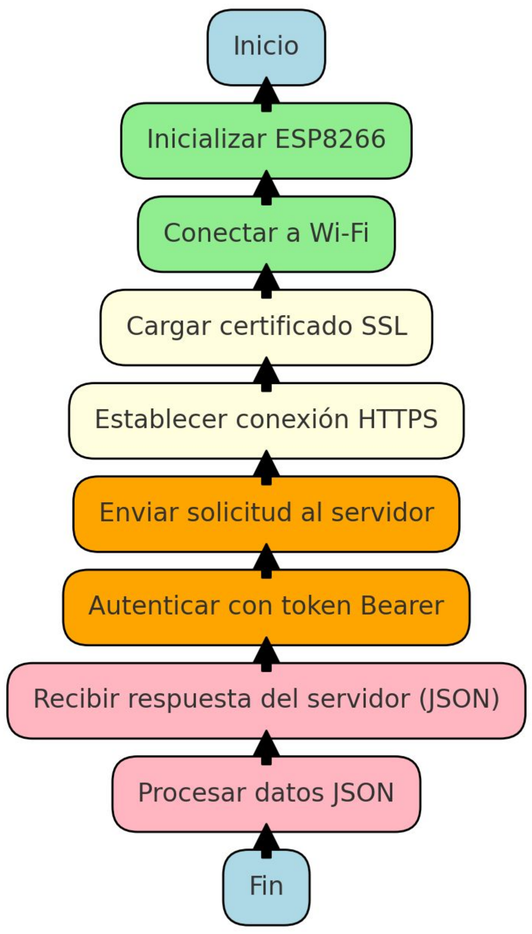
INTI, Av. Vélez Sársfield 1561, Córdoba., Argentina | jjorge@inti.gob.ar

1. Resumen del caso

Este proyecto utiliza un dispositivo ESP8266 para establecer una conexión segura mediante HTTPS con un servidor remoto. Está diseñado para recibir y procesar datos de sensores desplegados en el campo, garantizando la integridad de la información a través de la autenticación basada en tokens y el uso de protocolos de seguridad.

2. Situación inicial

La empresa cordobesa enfrentaba problemas con la precisión y seguridad de los datos que llegaban a sus servidores desde sensores remotos. Los sistemas originales no ofrecían mecanismos de protección contra posibles alteraciones o interferencias en la transmisión de datos. Esto generaba incertidumbre sobre la integridad de la información recibida. Era fundamental implementar una solución que asegurara que los datos enviados desde los sensores fueran auténticos y no se hubieran modificado durante su transmisión.



Secuencia de actividades que realiza el software.

3. Herramientas o métodos utilizados

Para realizar este proyecto se utilizaron:

ESP8266: microcontrolador Wi-Fi utilizado para enviar y recibir datos a través de redes inalámbricas, elegido por su bajo costo y capacidad de conexión a internet.

WiFiClientSecure: biblioteca utilizada para implementar conexiones HTTPS, asegurando que la comunicación entre el dispositivo y el servidor está cifrada. Es crucial usar HTTPS y no HTTP para proteger los datos contra ataques de intermediarios (man-in-the-middle) y garantizar que la información transmitida no sea interceptada ni manipulada.

Certificado SSL en formato PEM: utilizado para autenticar el servidor y asegurar la integridad y confidencialidad de la comunicación. La implementación de SSL/TLS asegura que solo el servidor legítimo puede recibir y descifrar los datos enviados.

NTP (Network Time Protocol): sincronización de tiempo mediante NTP es esencial para validar los certificados y asegurarse de que la autenticación basada en tiempo funcione correctamente. Se utiliza el servidor de tiempo NTP del INTI (Instituto Nacional de Tecnología Industrial) de Argentina, disponible en ntp.inti.gob.ar, para garantizar una referencia temporal precisa.

ArduinoJson: biblioteca utilizada para manejar y procesar las respuestas JSON enviadas por el servidor, permitiendo extraer y utilizar la información relevante de manera eficiente.

Autenticación basada en tokens "Bearer": implementación de un sistema de autenticación segura en el que el ESP8266 incluye un token "Bearer" en el encabezado de la solicitud. Esto garantiza que sólo los dispositivos autenticados puedan comunicarse con el servidor, evitando accesos no autorizados

La tecnología de comunicación segura basada en HTTPS tiene aplicaciones en una amplia gama de ámbitos más allá del monitoreo de sensores en el campo.

Automatización del hogar: el ESP8266 puede ser utilizado para controlar dispositivos domésticos inteligentes como luces, cerraduras, termostatos, cámaras, etc., desde cualquier lugar de manera segura. La autenticación y el cifrado HTTPS protegen los dispositivos de accesos no autorizados, garantizando la privacidad y seguridad.

Gestión de recursos: se puede aplicar en entornos urbanos, para monitorear y gestionar recursos como el consumo energético, el agua, o los residuos. Sensores conectados envían datos a servidores para un análisis eficiente, manteniendo siempre la seguridad de la información.

Telemedicina: los dispositivos basados en ESP8266 pueden recopilar datos de pacientes, como la presión arterial o el ritmo cardíaco, y enviarlos a médicos de forma remota. El uso de HTTPS garantiza que los datos médicos sensibles se transmitan de manera segura, cumpliendo con regulaciones como la HIPAA.

4. Resultados alcanzados

Se logró establecer una comunicación segura y confiable entre los sensores en campo y los servidores de la empresa en Córdoba. Gracias al uso de HTTPS, los datos enviados están protegidos contra modificaciones o interferencias. Además, la sincronización de tiempo mediante NTP garantiza la veracidad temporal de las conexiones, mientras que la autenticación por tokens asegura que sólo los dispositivos autorizados puedan interactuar con el servidor. Esta solución ha eliminado las dudas sobre la veracidad de los datos recibidos, proporcionando una infraestructura robusta para el monitoreo de sensores en tiempo real.

.

5. Prospectiva

Esta tecnología se puede aplicar en fábricas donde sensores conectados permiten el mantenimiento predictivo y el control de calidad de los procesos, asegurando la transmisión segura de datos a servidores remotos para optimización operativa. En el caso de dispositivos médicos pueden monitorear a los pacientes en tiempo real, enviando datos críticos a médicos de forma segura, cumpliendo con normativas de privacidad. En agricultura de precisión y sensores distribuidos en campos y ganado transmiten información vital sobre el clima, suelo o salud animal, mejorando la eficiencia agrícola a través de la seguridad en la transmisión de datos.