Tecnológico de Monterrey

Uso de Álgebras Modernas para Seguridad y Criptografía
Socio Formador: LiCore

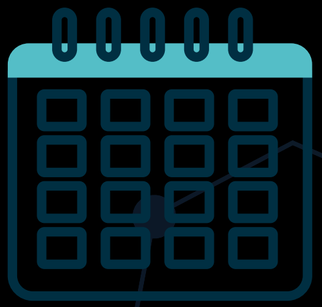
Lightweight Secure MQTT Broker:
Comunicación de dispositivos IoT en entornos de monitoreo y consumo de energía

Instituto Tecnológico y de Estudios Superiores de Monterrey
Escuela de Ingeniería y Ciencias
Ingeniería en Ciencias de Datos y Matemáticas
Monterrey, Nuevo León

16 de junio del 2023

Ricardo Camacho Castillo A01654132
Juan Pablo Echeagaray González A00830646
Daniela García Coindreau A00830236
Carolina Longoria Lozano A01721279
Michelle Yareni Morales Ramón A01552627
Emily Rebeca Méndez Cruz A00830768

Agenda



1. Introducción
2. Propuesta original
3. Cambios realizados
4. Live Demo
5. Next Steps
6. Round Table

Escenario

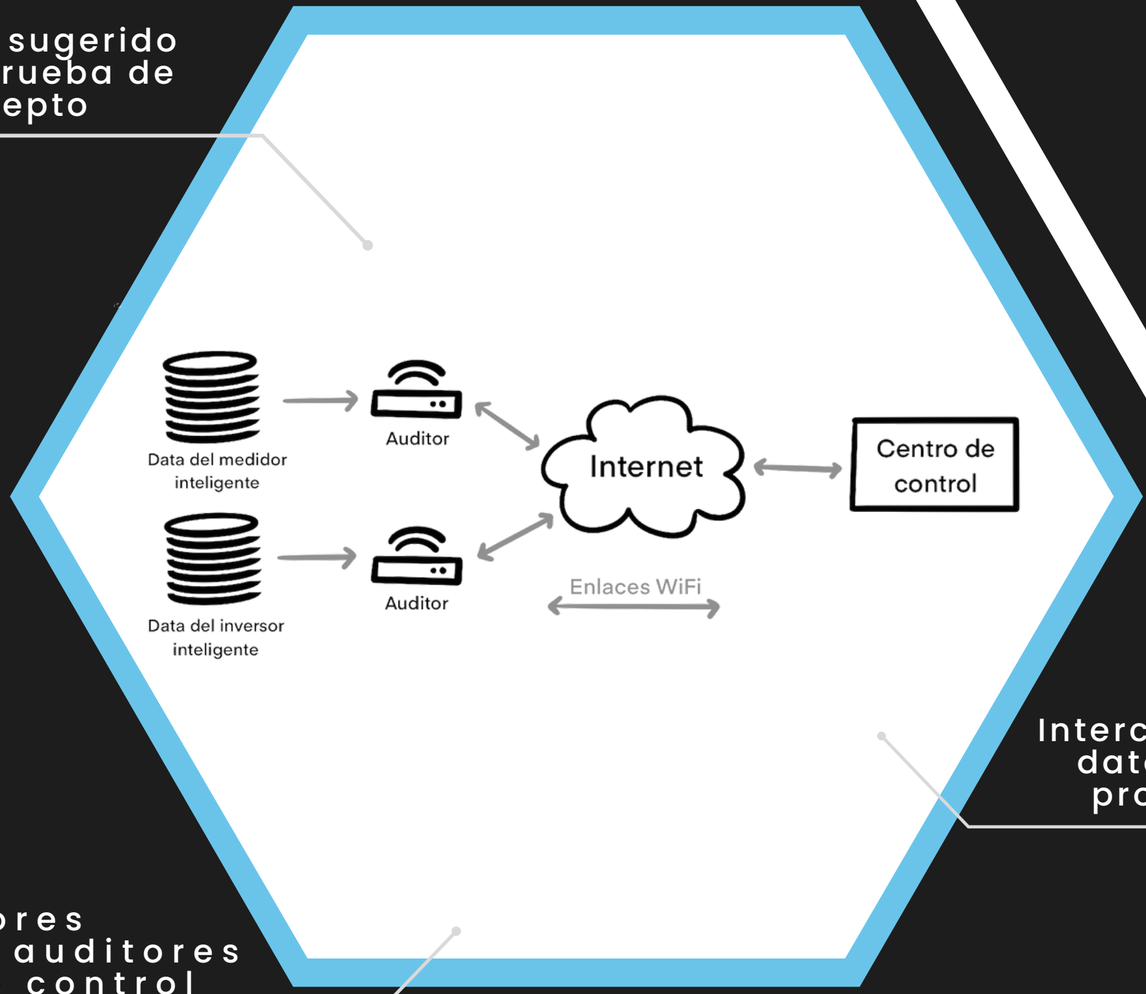
Objetivo

Implementar un protocolo de clave pública para un SmartGrid.

Desafíos

- Poder computacional restringido
- Comunicación en casi tiempo real
- Recursos económicos para contratar los dispositivos físicos y/o servicios
- Técnica a implementar para resguardar los datos

Esquema sugerido para la prueba de concepto



Intercambio de datos a ser protegido

Medidores inteligentes, auditores y centro de control

Justificación

Enfoque en Sostenibilidad

Innovar e industrializar sin sacrificar lo sostenible.

Acercar la energía al consumidor y con la elección de utilizar energías renovables.

Utilizar algoritmos ligeros que sean sostenibles y ayudar a que el proceso de producción de energía sostenible sea segura.

Dispositivos IoT

La interconexión IoT es uno de los principales desafíos debido a los recursos limitados. Por ello es importante la selección del dispositivo que fungirá como auditor.

Nombre	Chip	RAM	Disco Duro	Conectividad	OS	Lenguaje	Referencia
Raspberry Pi Model 3 B	ARM Cortex A53	1 GB	SD card	WiFi, Ethernet	Raspbian OS	Python, C++, etc...	[13]
ESP32	Tensilica Xtensa LX6	320 kB	448 KB Rom	WiFi, Bluetooth	-	Micropython, Circuit Python	[14]
Raspberry Pi Pico	Arm Cortex-M0+	264 kB	2 MB	WiFi	-	Micropython, C, C++	[15]

Listado de microcontroladores factibles

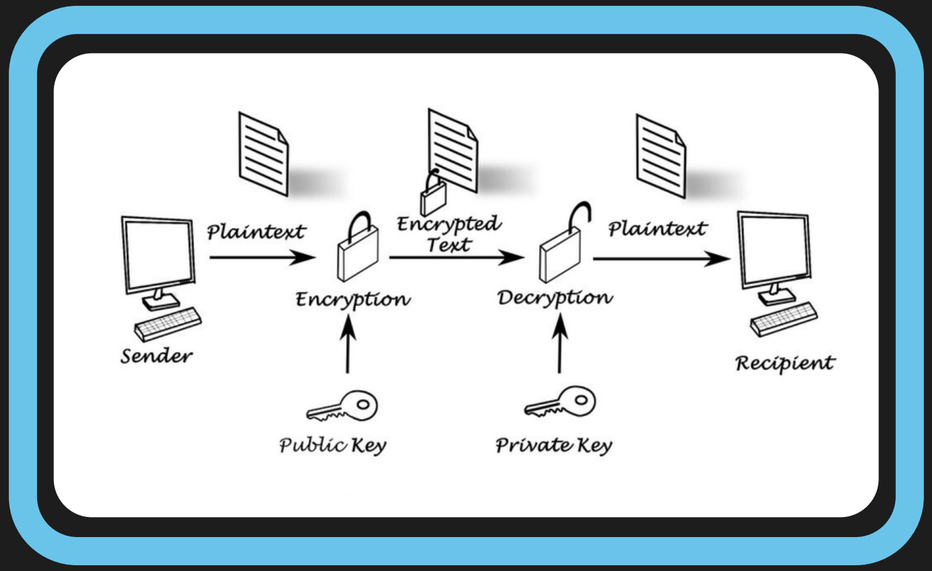
Encriptado

- Asimétrico

  RSA

  DSA

  ECDSA (método con mejor desempeño)



- Simétrico

  DES

  3DES

  AES128

  AES192

  AES256

Firma digital

Parte fundamental de los algoritmos encriptados es el *hash*. Algunas funciones de este tipo son:

- MD5
- SHA-1
- SHA-256
- SHA-512
- HAVAL
- KECCAK
- BLAKE

Protocolos criptográficos

1. Envío de datos por medio de HTTPS utilizando TLS.

2. Esquema de comunicación sobre MQTT incluyendo *hasheo* con firmado de claves públicas generadas de forma local.

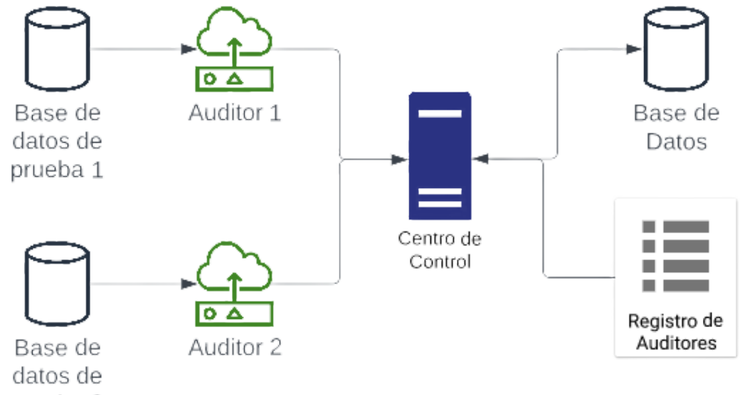
Propuesta original

01 Inicialización de parámetros

02 Selección de curva elíptica

03 Registro de dispositivos

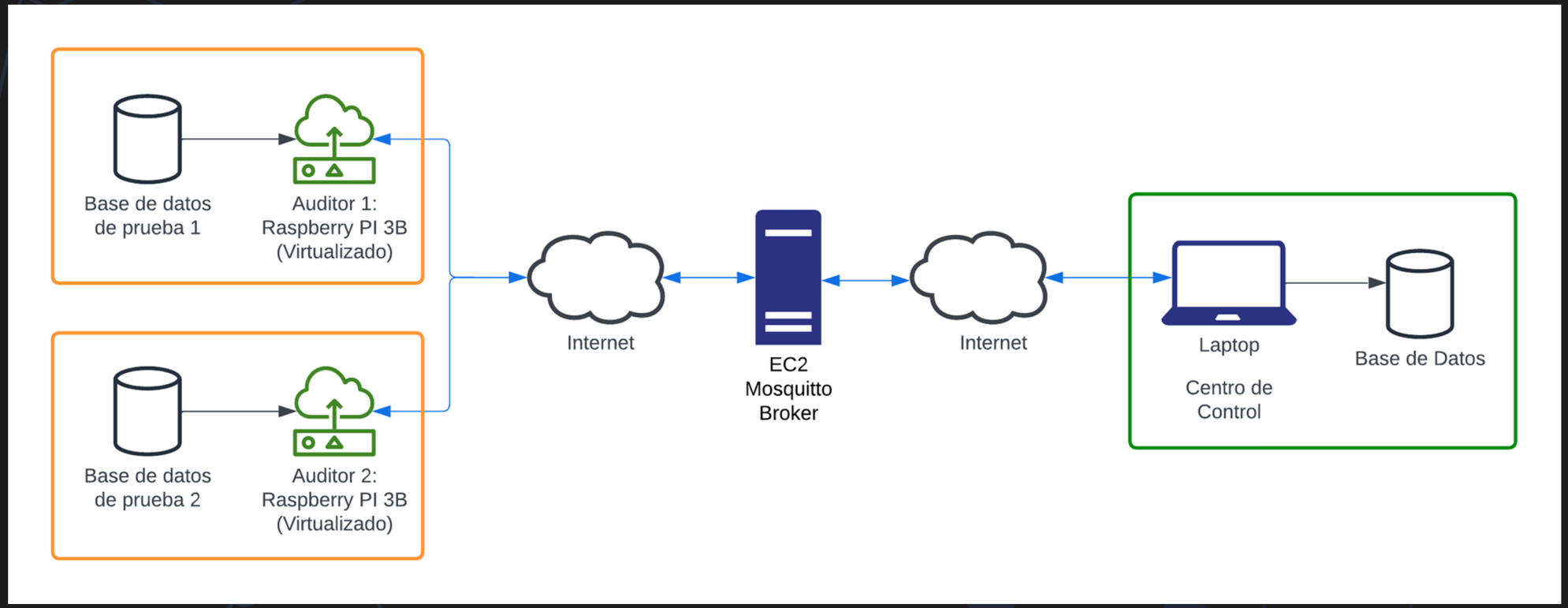
04 Autenticado e intercambio de datos

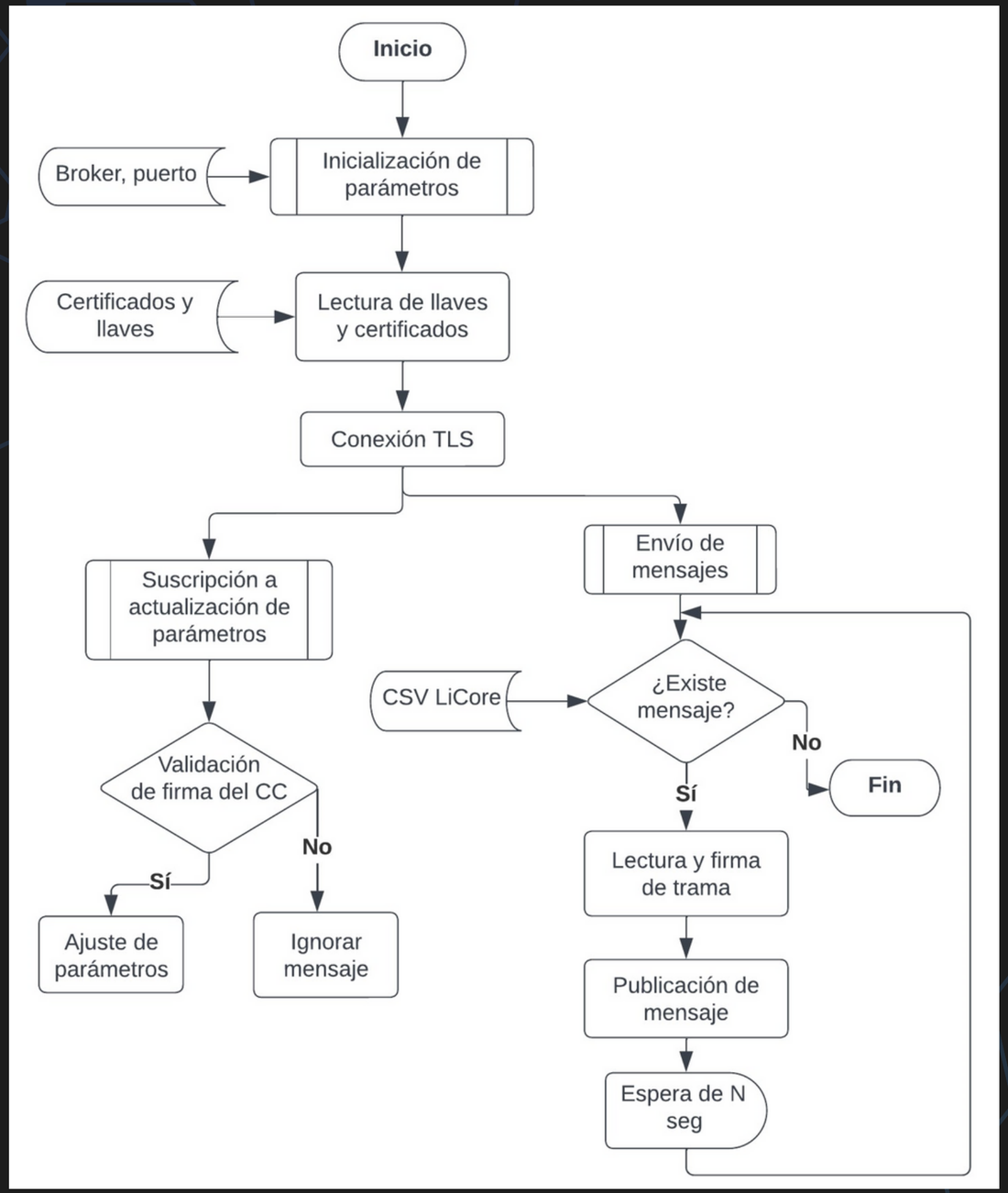


Cambios realizados

Cambios	Nuevo	Avances
1. No encriptado basado en HMAC 2. Separación de Broker y Centro de Control	1. Comunicación por TLS 2. Autenticación mediante ECDSA y BLAKE2	1. Comunicación bidireccional 2. Esquema de verificación de firmas 3. Rutina de procesamiento de tramas y guardado en base de datos 4. Simulación exitosa en entorno de pruebas

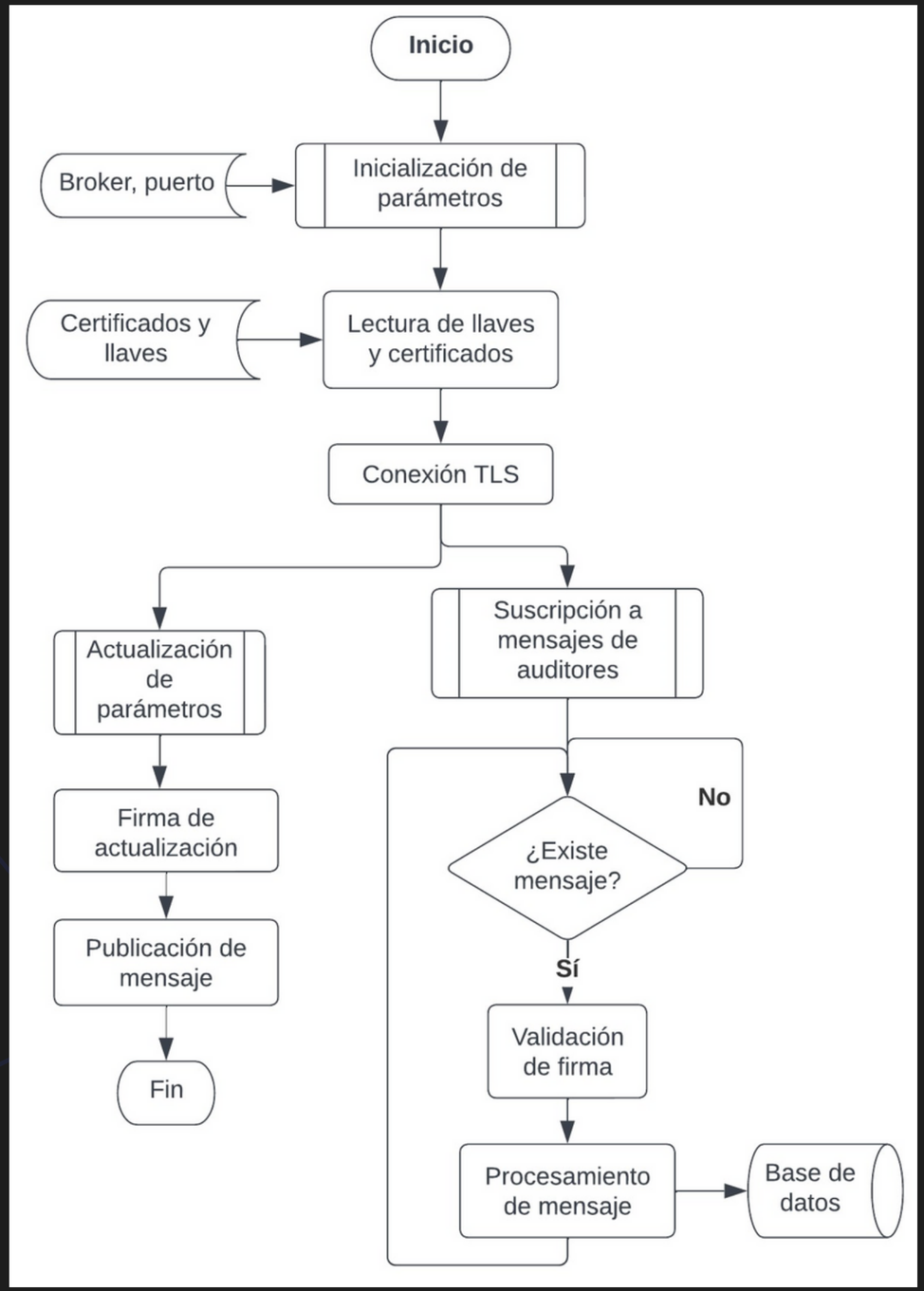
Nueva Arquitectura



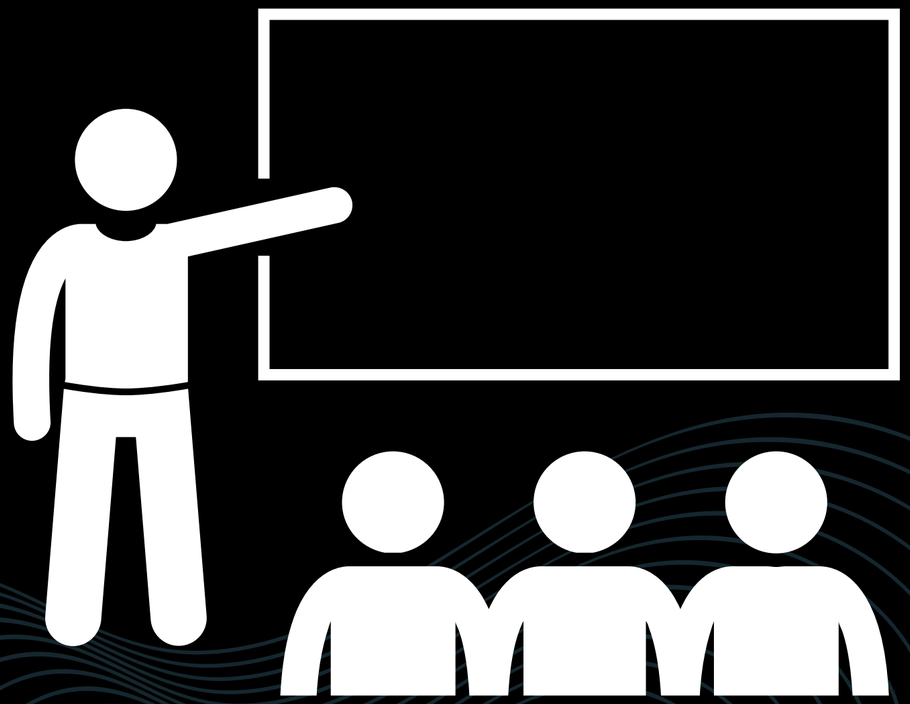


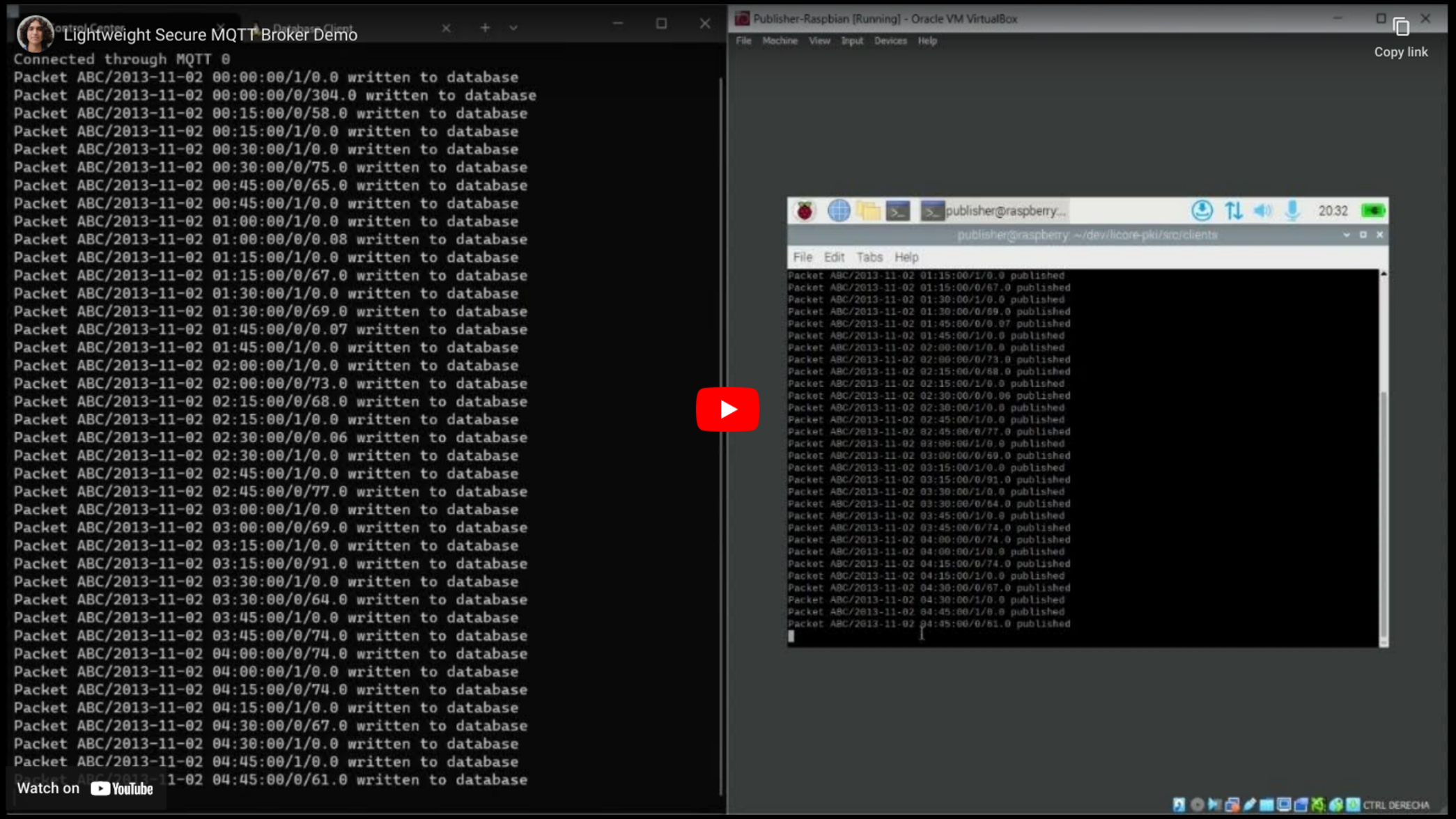
Flujo de mensajes: **Auditor**

Flujo de mensajes: Centro de Control



LIVE DEMO




Lightweight Secure MQTT Broker Demo
Copy link
Connected through MQTT 0
Packet ABC/2013-11-02 00:00:00/1/0.0 written to database
Packet ABC/2013-11-02 00:00:00/0/304.0 written to database
Packet ABC/2013-11-02 00:15:00/0/58.0 written to database
Packet ABC/2013-11-02 00:15:00/1/0.0 written to database
Packet ABC/2013-11-02 00:30:00/1/0.0 written to database
Packet ABC/2013-11-02 00:30:00/0/75.0 written to database
Packet ABC/2013-11-02 00:45:00/0/65.0 written to database
Packet ABC/2013-11-02 00:45:00/1/0.0 written to database
Packet ABC/2013-11-02 01:00:00/1/0.0 written to database
Packet ABC/2013-11-02 01:00:00/0/0.08 written to database
Packet ABC/2013-11-02 01:15:00/1/0.0 written to database
Packet ABC/2013-11-02 01:15:00/0/67.0 written to database
Packet ABC/2013-11-02 01:30:00/1/0.0 written to database
Packet ABC/2013-11-02 01:30:00/0/69.0 written to database
Packet ABC/2013-11-02 01:45:00/0/0.07 written to database
Packet ABC/2013-11-02 01:45:00/1/0.0 written to database
Packet ABC/2013-11-02 02:00:00/1/0.0 written to database
Packet ABC/2013-11-02 02:00:00/0/73.0 written to database
Packet ABC/2013-11-02 02:15:00/0/68.0 written to database
Packet ABC/2013-11-02 02:15:00/1/0.0 written to database
Packet ABC/2013-11-02 02:30:00/0/0.06 written to database
Packet ABC/2013-11-02 02:30:00/1/0.0 written to database
Packet ABC/2013-11-02 02:45:00/1/0.0 written to database
Packet ABC/2013-11-02 02:45:00/0/77.0 written to database
Packet ABC/2013-11-02 03:00:00/1/0.0 written to database
Packet ABC/2013-11-02 03:00:00/0/69.0 written to database
Packet ABC/2013-11-02 03:15:00/1/0.0 written to database
Packet ABC/2013-11-02 03:15:00/0/91.0 written to database
Packet ABC/2013-11-02 03:30:00/1/0.0 written to database
Packet ABC/2013-11-02 03:30:00/0/64.0 written to database
Packet ABC/2013-11-02 03:45:00/1/0.0 written to database
Packet ABC/2013-11-02 03:45:00/0/74.0 written to database
Packet ABC/2013-11-02 04:00:00/0/74.0 written to database
Packet ABC/2013-11-02 04:00:00/1/0.0 written to database
Packet ABC/2013-11-02 04:15:00/0/74.0 written to database
Packet ABC/2013-11-02 04:15:00/1/0.0 written to database
Packet ABC/2013-11-02 04:30:00/0/67.0 written to database
Packet ABC/2013-11-02 04:30:00/1/0.0 written to database
Packet ABC/2013-11-02 04:45:00/1/0.0 written to database
1-02 04:45:00/0/61.0 written to database
Watch on YouTube
Publisher-Raspbian [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
publisher@raspberry...
20:32
publisher@raspberry: ~/dev/licore-pki/src/clients
File Edit Tabs Help
Packet ABC/2013-11-02 01:15:00/1/0.0 published
Packet ABC/2013-11-02 01:15:00/0/67.0 published
Packet ABC/2013-11-02 01:30:00/1/0.0 published
Packet ABC/2013-11-02 01:30:00/0/69.0 published
Packet ABC/2013-11-02 01:45:00/0/0.07 published
Packet ABC/2013-11-02 01:45:00/1/0.0 published
Packet ABC/2013-11-02 02:00:00/1/0.0 published
Packet ABC/2013-11-02 02:00:00/0/73.0 published
Packet ABC/2013-11-02 02:15:00/0/68.0 published
Packet ABC/2013-11-02 02:15:00/1/0.0 published
Packet ABC/2013-11-02 02:30:00/0/0.06 published
Packet ABC/2013-11-02 02:30:00/1/0.0 published
Packet ABC/2013-11-02 02:45:00/1/0.0 published
Packet ABC/2013-11-02 02:45:00/0/77.0 published
Packet ABC/2013-11-02 03:00:00/1/0.0 published
Packet ABC/2013-11-02 03:00:00/0/69.0 published
Packet ABC/2013-11-02 03:15:00/1/0.0 published
Packet ABC/2013-11-02 03:15:00/0/91.0 published
Packet ABC/2013-11-02 03:30:00/1/0.0 published
Packet ABC/2013-11-02 03:30:00/0/64.0 published
Packet ABC/2013-11-02 03:45:00/1/0.0 published
Packet ABC/2013-11-02 03:45:00/0/74.0 published
Packet ABC/2013-11-02 04:00:00/0/74.0 published
Packet ABC/2013-11-02 04:00:00/1/0.0 published
Packet ABC/2013-11-02 04:15:00/0/74.0 published
Packet ABC/2013-11-02 04:15:00/1/0.0 published
Packet ABC/2013-11-02 04:30:00/0/67.0 published
Packet ABC/2013-11-02 04:30:00/1/0.0 published
Packet ABC/2013-11-02 04:45:00/1/0.0 published
Packet ABC/2013-11-02 04:45:00/0/61.0 published
CTRL DERECHA

Next Steps

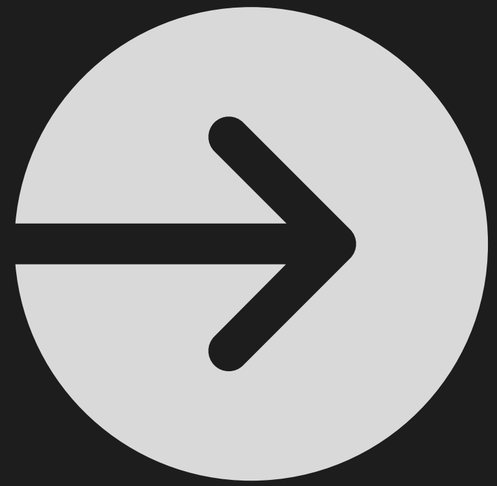
01 Preparación de documentación oficial

02 Conexion de instancia con VS Code

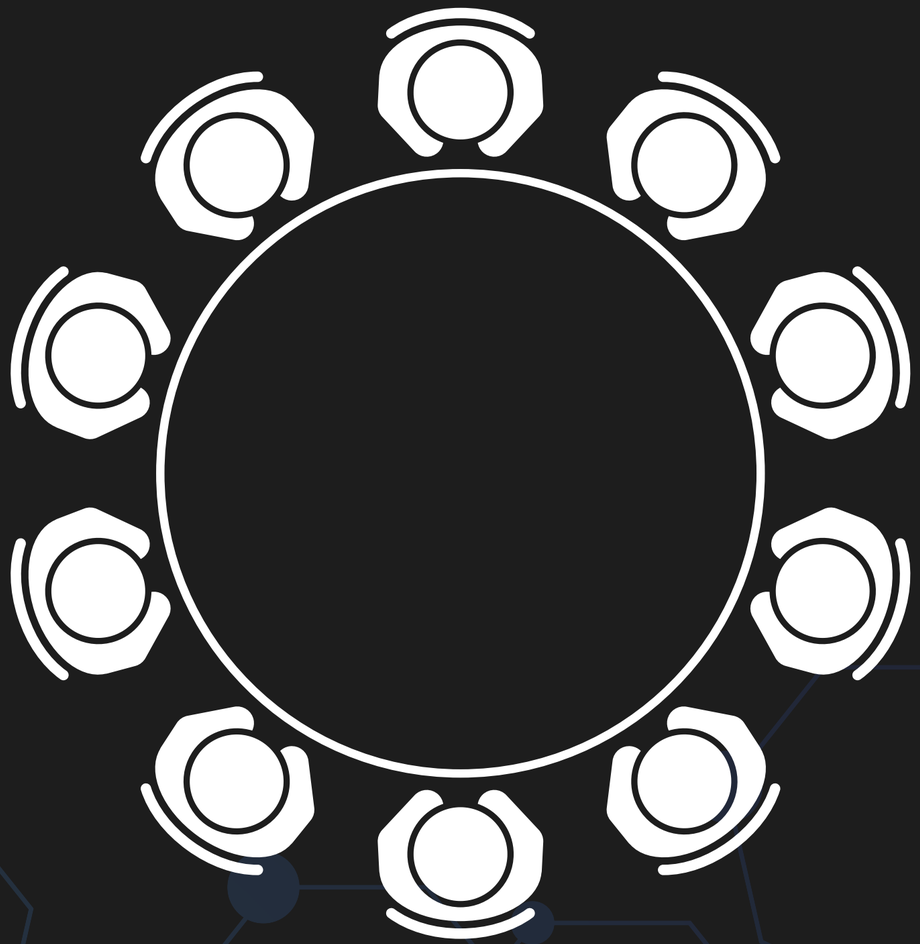
03 Creación de certificados por lotes

04 Refactoring general del código desarrollado

05 Uso de Amazon S3 Bucket para el almacenamiento de datos



Round Table



Referencias

M. El-Haii, M. Chamoun, A. Fadlallah, and A. Serhrouchni, “Analysis of cryptographic algorithms on iot hardware platforms,” in 2018 2nd Cyber Security in Networking Conference (CSNet). IEEE, 2018, pp. 1–5.

A. Anand, A. Galletta, A. Celesti, M. Fazio, and M. Villari, “A secure inter-domain communication for iot devices,” in 2019 IEEE International Conference on Cloud Engineering (IC2E). IEEE, 2019, pp. 235–240.

R. P. Ltd, “Buy a Raspberry Pi Pico - Raspberry Pi.” [Online]. Available: https://www.raspberrypi.com/products/raspberry-pi-pico/

“NVD - CVE-2016-2183.” [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2016-2183

“What is MD5? Understanding Message-Digest Algorithms — Okta.” [Online]. Available: https://www.okta.com/identity-101/md5/

“NIST Retires SHA-1 Cryptographic Algorithm — NIST,” 12 2022. [Online]. Available: https://www.nist.gov/news-events/news/2022/12/nist-retires-sha-1-cryptographic-algorithm

V. Rao and K. Prema, “Comparative study of lightweight hashing functions for resource constrained devices of iot,” in 2019 4th International Conference on Computational Systems and Information Technology for Sustainable Solution (CSITSS), vol. 4. IEEE, 2019, pp. 1–5.

V. Abreu, A. O. Santin, E. K. Viegas, and V. V. Cogo, “Identity and access management for iot in smart grid,” in Advanced Information Networking and Applications: Proceedings of the 34th International Conference on Advanced Information Networking and Applications (AINA-2020). Springer, 2020, pp. 1215–1226.

A. Lohachab et al., “Ecc based inter-device authentication and authorization scheme using mqtt for it networks,” Journal of Information Security and Applications, vol. 46, pp. 1–12, 2019.