Implementación de criptografía de clave pública para protección de comunicaciones y almacenamiento de datos con IoT en entornos de monitoreo y consumo de energía.

Instituto Tecnológico y de Estudios Superiores de Monterrey

Escuela de Ingeniería y Ciencias

Ingeniería en Ciencia de Datos y Matemáticas

Uso de Álgebras Modernas para Seguridad y Criptografía

LiCore

Monterrey, Nuevo León

Junio 16, 2023

Andrea Bravo Avila A01028579
Renata Vargas Caballero A01025281
Natalia Monserrat González de León A00831090
Fernando González Rosas A01253694
Alberto Lozano Cárdenas A01067141
Fernanda Sherlin Calderón López A01275430
Gil Herzberg Alperon A00827347

Agenda

01

Planteamiento

02

Solución Propuesta

03

Descripción de la Solución

04

Resultados Obtenidos

05

Conclusiones y trabajo futuro

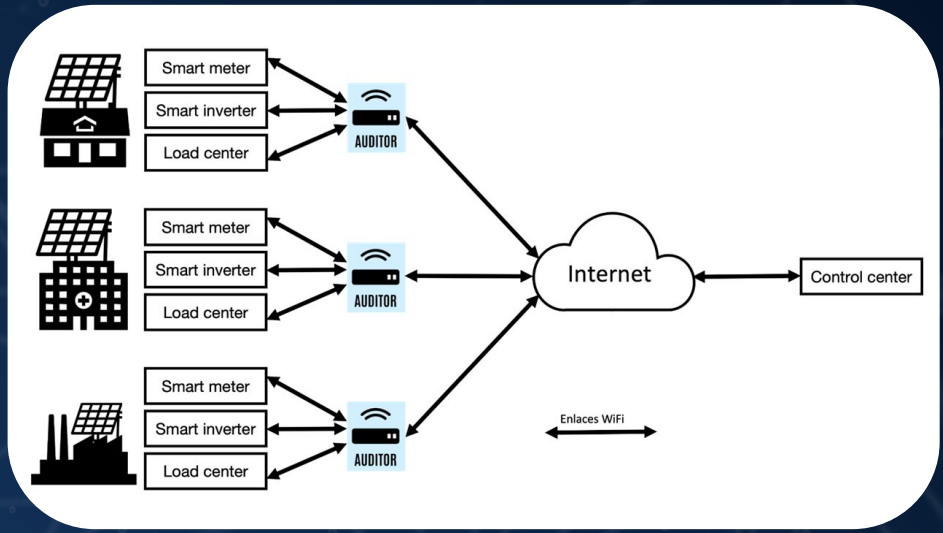
06

Referencias

01
Planteamiento

LiCORE y datos seguros

- Confidencialidad
- Identidad
- Autenticidad

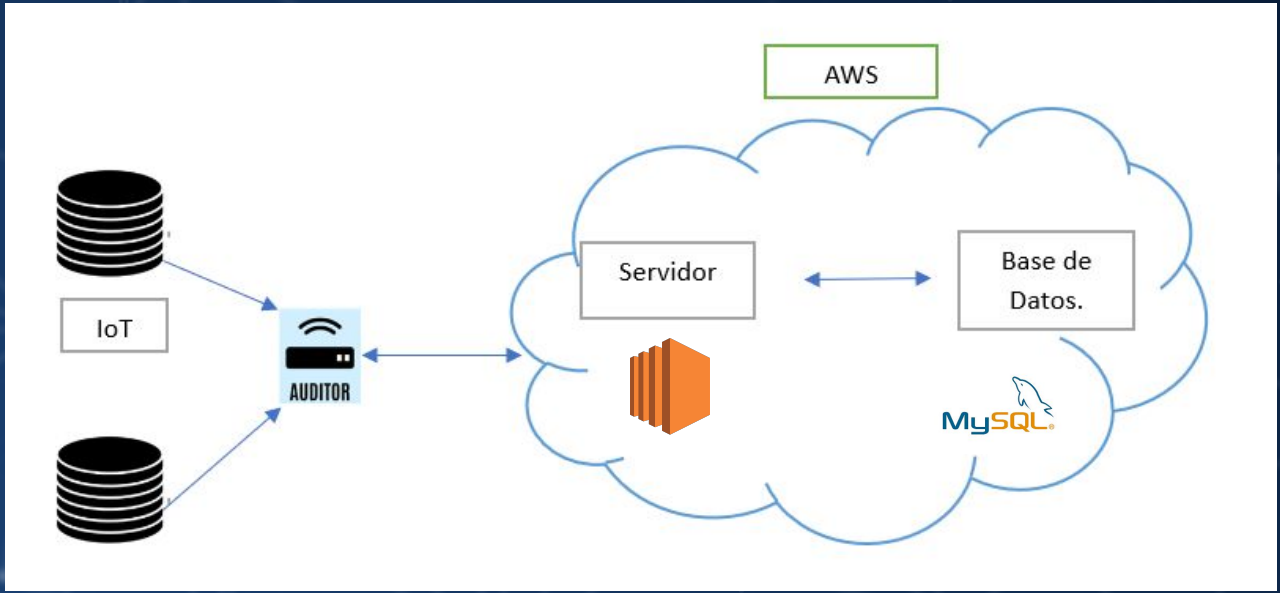


Canvas, Camero H

02

Solución Propuesta

Arquitectura



- Raspberry Pi 3
- Amazon Web Services:
  - RDS
  - EC2
- Diversas librerías de Python.

03
Descripción de la Solución

Componentes principales

AWS

Una plataforma de computación en la nube que ofrece una amplia gama de servicios escalables y flexibles para almacenamiento, potencia de cálculo, gestión de bases de datos y más.

Flask

Un framework ligero y flexible de Python para desarrollar aplicaciones web rápidas y eficientes, con una sintaxis sencilla y amplia comunidad de soporte.

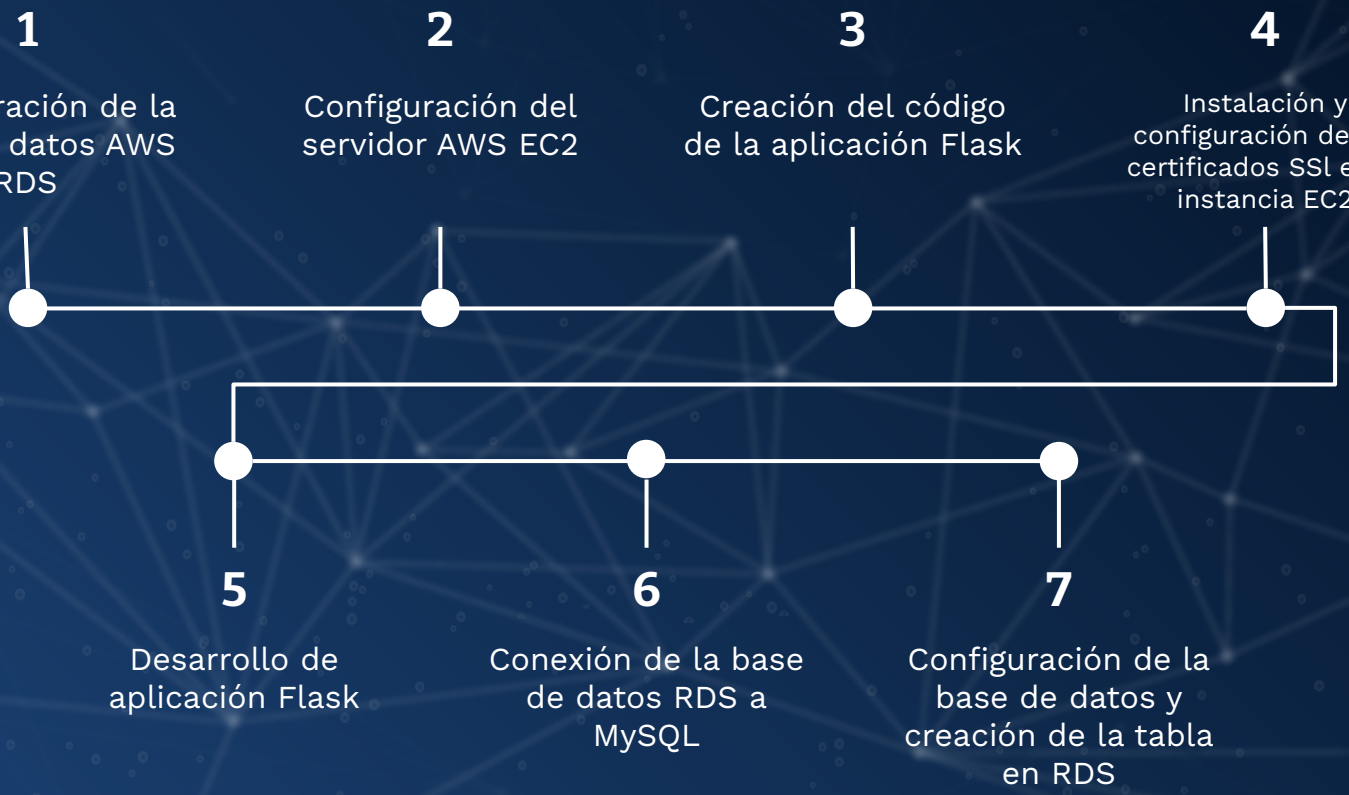
SSL en EC2

Es un protocolo de seguridad que cifra la comunicación entre un servidor web y un cliente, garantizando la confidencialidad y autenticidad de los datos transmitidos.

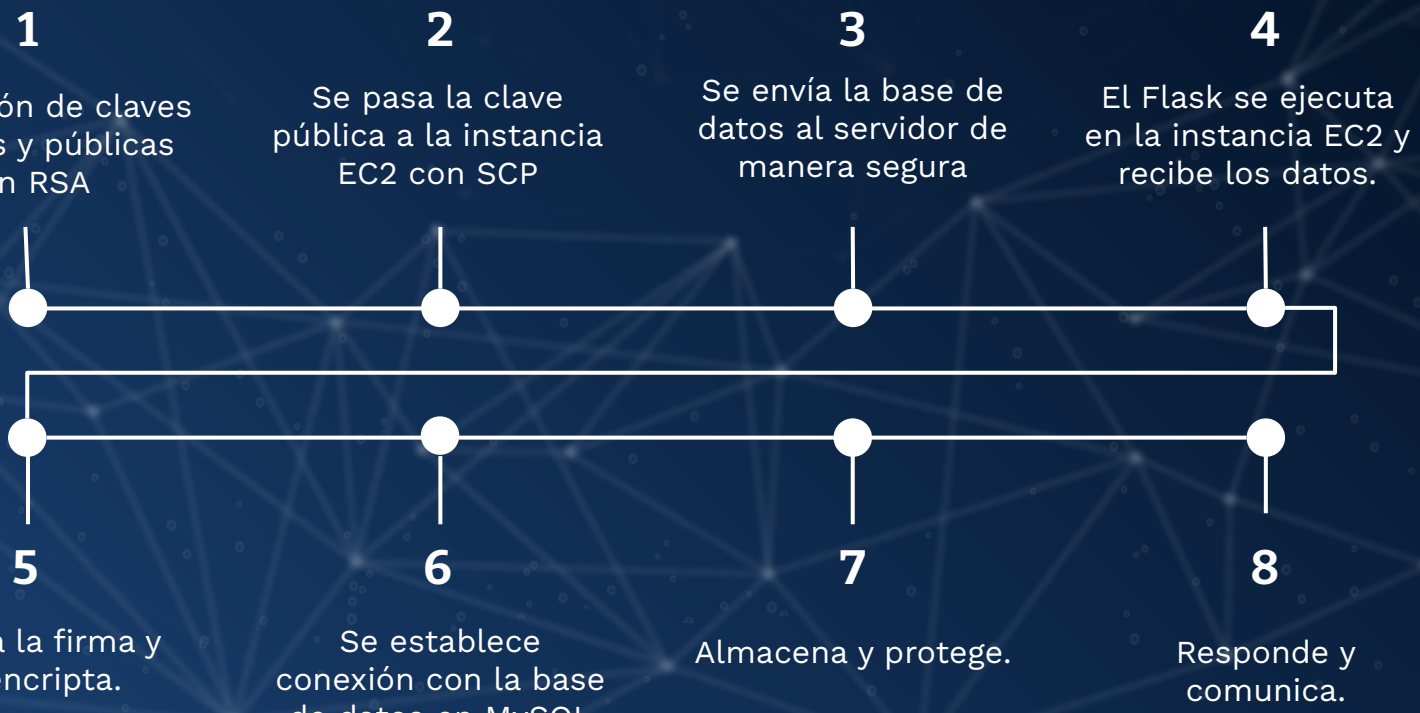
EC2

Servicio de AWS que proporciona servidores virtuales escalables y configurables según la demanda, permitiendo ejecutar aplicaciones en la nube de manera eficiente y económica.

Estructura y Configuración



Paso a Paso Raspberry



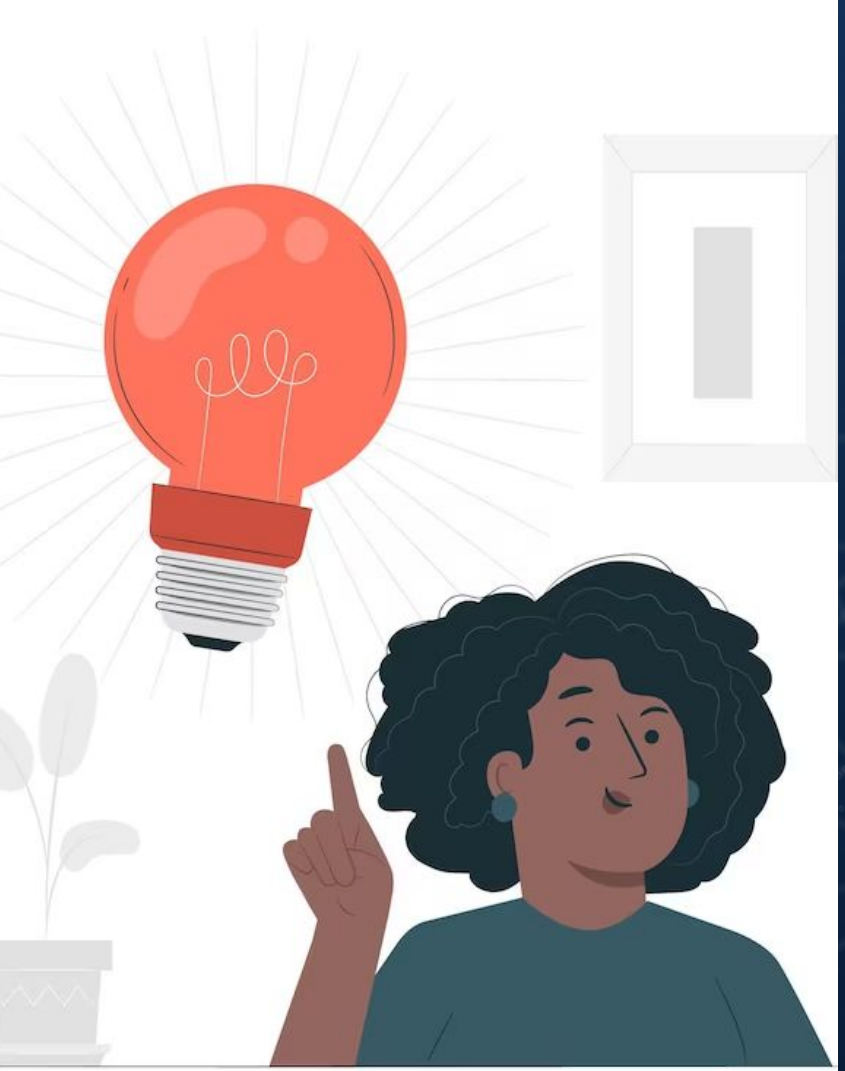
04
Resultados Obtenidos

Sistema IOT

```
(base) C:\Users\gilhe>cd claves

(base) C:\Users\gilhe\claves>ssh claves_proyecto.pem ec2-user@17.191.206.122
ssh: Could not resolve hostname claves_proyecto.pem: Host desconocido.

(base) C:\Users\gilhe\claves>ssh -i claves_proyecto.pem ec2-user@18.191.206.122
Last login: Mon Jun 12 19:29:36 2023 from fixed-187-189-163-4.totalplay.net

       __|  __|_  )
       _|  (     /   Amazon Linux 2 AMI
      ___|\___|___|

https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-172-31-18-118 ~]$ cd flask_app
[ec2-user@ip-172-31-18-118 flask_app]$ python3 prueba.py
[{'EntryID': 1, 'ID': 'ABC', 'ConsumptionOrProduction': 0, 'Day': 2, 'Month': 11, 'Year': 2013, 'Time': datetime.timedel
ta(0), 'Reading': 58.0}, {'EntryID': 2, 'ID': 'ABC', 'ConsumptionOrProduction': 1, 'Day': 2, 'Month': 11, 'Year': 2013,
'Time': datetime.timedelta(0), 'Reading': 0.0}, {'EntryID': 3, 'ID': 'ABC', 'ConsumptionOrProduction': 0, 'Day': 2, 'Mon
th': 11, 'Year': 2013, 'Time': datetime.timedelta(seconds=900), 'Reading': 75.0}, {'EntryID': 4, 'ID': 'ABC', 'Consumpti
onOrProduction': 1, 'Day': 2, 'Month': 11, 'Year': 2013, 'Time': datetime.timedelta(seconds=900), 'Reading': 0.0}, {'Ent
ryID': 5, 'ID': 'ABC', 'ConsumptionOrProduction': 0, 'Day': 2, 'Month': 11, 'Year': 2013, 'Time': datetime.timedelta(sec
onds=1800), 'Reading': 65.0}]
[ec2-user@ip-172-31-18-118 flask_app]$ python3 borrar_registros.py
[ec2-user@ip-172-31-18-118 flask_app]$ python3 prueba.py
()
```

```
EntryID,ID,ConsumptionOrProduction,Day,Month,Year,Time,Reading
1,0,0,2,11,2013,00:00:00,58
2,0,1,2,11,2013,00:00:00,0
3,0,0,2,11,2013,00:15:00,75
4,0,1,2,11,2013,00:15:00,0
```

- **Q1**
  El sistema funciona
- **Q2**
  Encripta y firma
- **Q3**
  Desencripta y verifica
- **Q4**
  Almacena y protege



05
Conclusiones y trabajo futuro

FIN

06
Referencias

Referencias

[1] Gómez, J. S. (2004). Criptografıa de clave pública: El sistema rsa. Sigma: revista de matemáticas= matematika aldizkaria, (25), 149–165

[2] KeepCoding. (2022). ¿qué es el algoritmo diffie-hellman? https://keepcoding.io/blog/que-es-el-algoritmo-diffie-hellman/

[3] ElGamal, T. (1985). A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE transactions on information theory, 31(4), 469-472.

[4] Sánchez Martın, J.A. (2021). Solución de cifrado para dispositivos de bajas capacidades.

[5] Cisco. (2023). ¿qué es una vpn? - red privada virtual. https://www.cisco.com/c/es mx/products/security/vpn- endpoint- security- clients/what- is-vpn.html

[6] Diana, H. (2021). Red de área local o lan. https://www.computerweekly.com/es/definicion/Red-de-area-local-o-LAN

[7] European Knowledge Center for Information Technology. (2018). Red de ´ area amplia (WAN). https://www.ticportal.es/glosario-tic/wan-red-area-amplia

[8] Vintró, J. (2005). Redes y acceso a internet. ELSEVIER. https://www.elsevier.es/es-revista-offarm-4-articulo-redes-acceso-internet-13075590

[9] Roberto, R. (2021). Medios de transmisión para redes inalámbricas. Universidad Autónoma de Coahuila, 1–3.

[10] Arduino. (2014). Arduino uno rev3. Arduino https://store.arduino.cc/usa/arduino-uno-rev3

[11] Foundation, R. P. (2019). Raspberry pi 4 model b. Raspberry Pi Foundation.https://www.raspberrypi.org/products/raspberry-pi-4-model-b/