Instituto Tecnológico y de Estudios Superiores de Monterrey

Escuela de Ingeniería y Ciencias

Ingeniería en Ciencias de Datos y Matemáticas

Uso de álgebras modernas para seguridad y criptografía

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

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

Dr. Alberto F. Martínez

Dr. Daniel Otero Fadul

Socio Formador: COCOA, LICORE

Monterrey, Nuevo León

17 de marzo del 2023

Índice

Índice de figuras

Índice de cuadros

1. Introducción

Mientras avanzamos en el camino de la industrialización, los datos se vuelven más y más vitales para el funcionamiento de cualquier empresa. Más allá de ser de suma importancia para el análisis de su rendimiento, muchas veces fungen como materia prima de sus procesos. Las fugas de información no son necesariamente nuevas, pero la era digital ha permitido que ocurran de una manera masiva, y ha llegado a afectar a empresas renombradas como Yahoo, Microsoft y Facebook [1]. Muchas veces estas empresas manejan datos sensibles, y una filtración de datos es un problema grave para ellos y sus usuarios.

Este es el caso para nuestros socios formadores, *Cocoa* y *LiCore*. *Cocoa* se enfoca en facilitar la transición energías limpias utilizando herramientas digitales [2], y *LiCore* se enfoca en desarrollar tecnología electrónica en áreas relacionadas a la energía sostenible. Una parte clave en su proceso consiste en documentar información de la cantidad y calidad de la energía, que al obtenerse pasa a un auditor, y del auditor a un centro de control. Estos datos al ser de carácter sensible, necesitan ser transmitidos por un medio seguro, por lo que es imperativo la implementación de un medio de transporte seguro que se adapte a los dispositivos que utiliza el Socio Formador.

A continuación estableceremos el objeto de nuestro estudio, plantearemos el problema a ser solucionado y elaboraremos una justificación. Después, haremos una investigación extensa sobre el estado del arte. Analizaremos los recursos disponibles para la resolución del problema, y nuestros objetivos para solucionarlo. Determinaremos la arquitectura de red a ser utilizada y propondremos nuestra metodología. Finalmente, discutiremos los resultados obtenidos.

2. Objeto de estudio

El caso de estudio general que compete a un proyecto como el presentado es la implementación de un protocolo de clave pública para un *SmartGrid*, que es equivalente a una red heterogénea de dispositivos IoT [3].

La implementación de dicha arquitectura viene de la mano con un conjunto de desafíos asociados al poder computacional restringido de los dispositivos IoT, la necesidad de que la comunicación entre los miembros de la red suceda casi en tiempo real, en la disponibilidad de recursos económicos para la construcción y selección de los dispositivos físicos y/o servicios a contratar, y en la técnica a implementar para resguardar los datos de los auditores en una base de datos segura.

Los datos a enviar serán de carácter energético, conteniendo información del consumo y generación de energía eléctrica asociados a un domicilio y a una etiqueta de tiempo. Los datos generados son de carácter sensible, pues algún agente malicioso podría utilizar algún método de *spyware* para recolectar dichos datos, realizar algún proceso de caracterización para lanzar un ataque acotado y personalizado a los entes asociados al conjunto de datos vulnerados.

3. Planteamiento del problema

3.1. Descripción general de la problemática

En la Figura 1 se muestra un esquema simplificado más general de la red *SmartGrid* que se busca asegurar. En primera instancia, se busca proteger el intercambio de información entre cada auditor y el control center. Se busca asegurar la confidencialidad, integridad y autenticidad en todo el proceso de comunicación para que solamente los dispositivos autorizados por el centro deo control puedan publicar y acceder a los datos medidos, que la información medida no sufra de alteración alguna y que existan los medios suficientes para aplicar un criterio de no repudio a los auditores participantes de la red.

En conjunto con la Figura 1, se proporciona la Tabla 3.1 en la que se enumera y describen las labores de los componentes básicos de la red solicitada por el Socio Formador.

Componente	Función	Dispositivo
SmartMeter	Monitoreo de parámetros de consumo y generación de energía eléctrica, envío de datos medidos a su auditor respectivo por medio de WiFi	No aplica
Auditor	Recolección de datos de SmartMeters, envío de datos al centro de control	Microcontroladores, tarjetas tipo Raspberry Pi
Centro de control	Procesamiento de lecturas enviadas por auditores, respaldo encriptado de mediciones en una base de datos	Servidor en la nube

Tabla 1: Listado general de los componentes de la red

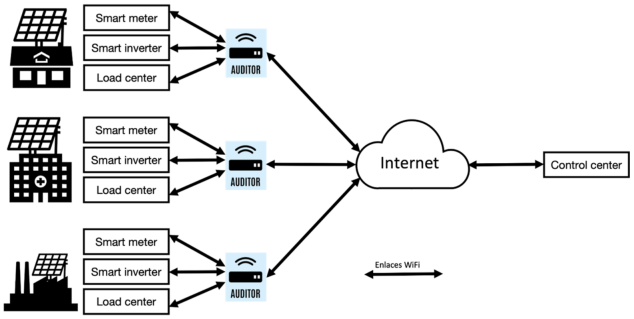

Figura 1: Intercambio de Datos a ser Protegido [Extraído de CANVAS]

3.2. Delimitación del problema

Para fines académicos a organización socio-formadora propone el escenario representado en la Figura 2. Se dispondrá de dos auditores, que reportan el consumo y generación de energía eléctrica de 2 residencias

distintas. Los datos en cuestión no serán obtenidos en tiempo real, sino que han sido proporcionados por el socio-formador en el formato de un archivo csv con los registros históricos de las mediciones.

Los datos recolectados por los auditores deben de ser enviados por internet protegidos hasta que lleguen al Centro de Control. En el Centro de Control, los datos serán almacenados en una base de datos en donde serán respaldados con un esquema de encriptado seguro.

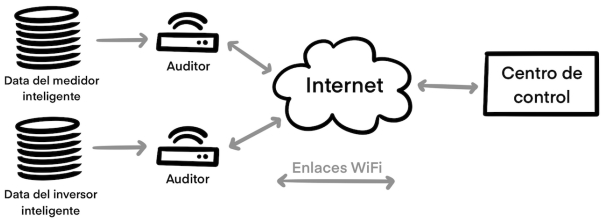

Figura 2: Esquema sugerido para la prueba de concepto (PdC).[Imagen referenciada de CANVAS]

4. Justificación

4.1. Enfoque en Sostenibilidad

Nuestro propósito se alinea con múltiples de los Objetivos de Desarrollo Sustentable de las ONU.

- **Objetivo 9**: «Construir infraestructuras resilientes, promover la industrialización sostenible y fomentar la innovación.» [4] Lo vemos reflejado en nuestro deseo de innovar e industrializar sin sacrificar lo sostenible.
- **Objetivo 11**: «Lograr que las ciudades sean más inclusivas, seguras, resilientes y sostenibles.» [5] Este objetivo esta integrado en las bases del proyecto, con la intención del socio formador de acercar la energía al consumidor, y con su elección de utilizar energías renovables.
- **Objetivo 12**: «Garantizar modalidades de consumo y producción sostenibles.»[6] Es uno de nuestros principales enfoques, al utilizar algoritmos ligeros que serán lo mas sostenibles posibles, y al ayudar a que un proceso de producción de energía sostenible pueda efectuar de manera segura.

4.2. Dimensión legal y económica

De acuerdo a IBM, el costo global promedio en 2022 de una filtración de datos fue de 4 millones de dólares [7]. Esta cifra sigue un patrón de aumento a través del tiempo, lo que nos indica que cada vez se vuelve más caro tener datos desprotegidos. Lo económico no es lo único que se ve afectado por un ataque de esta naturaleza. El estudio del Instituto Ponmeon, "The Aftermath of a Mega Data Breach: Consumer Sentiment", clasifica a las filtraciones de datos como el tercer factor más influyente para la reputación de una empresa, junto con desastres naturales y mal servicio al cliente [8].

Cada segundo se conectan a internet alrededor de 127 dispositivos nuevos. Estos dispositivos atraen a ciberdelicuentes debido a que muchas de las personas que compran dichos aparatos desconocen los puntos importantes de ciberseguridad al momento de adquirirlo, el cual puede poner en riesgo la privacidad del usuario. Los dispositivos IoT usualmente son objetivo de ataques forzados. Los ataques forzados usando motores de búsqueda especializados en donde se seleccionan equipos de protocolos disponibles para conexión, así forzando de manera automática los nombres de usuario y contraseñas comunes. Se estima que a nivel global, la cifra de ataques a dispositivos IoT es mayor a los mil 500 millones. En México, el primer semestre de 2021 se detectaron 661 mil 715 ataques a dispositivos IoT [9]. La cantidad de ataques tuvo un incremento de 197 por ciento a comparación con el año 2020 en donde se registran 222 mil 599.

Como se ha mencionado anteriormente los ataques a dispositivos IoT son comunes y costosos, a continuación se describirán algunos ataques o vulnerabilidades encontradas en dispositivos por el mal uso de primitivas criptográficas:

- En noviembre 2016, cibercriminales apagaron la calefacción de dos edificios en la ciudad finlandesa de Lappeenranta. Después de este ataque, se lanzó un segundo ataque DDoS, en donde obligaron a los controladores de calefacción a reiniciar el sistema repetidamente así evitando que la calefacción se encendiera. Este fue un ataque severo ya que en Finlandia se experimentan temperaturas muy bajas en esa época del año [10].

- En el 2016, investigadores encontraron que alrededor de 100 millones de vehículos Volkswagen vendidos desde 1995 pueden ser atacados por cibercriminales con una facilidad relativa para abrir puertas de forma inalámbrica sin tener la llave. Los vehículos eran vulnerable debido a que se usaron una mínima cantidad de claves privadas compartidas, en donde una vez que se viole una sola clave privada entonces millones de vehículos se verán comprometidos ya que los 100 millones de vehículos y sus llaveros fueron programados con pocas claves secretas comunes utilizadas en todo el mundo. Esto comprometía la seguridad de los pasajeros ya que ellos suponen que el vehículo esta bien cerrado comprometiéndolos a un robo en la carretera, a que criminales coloquen discretamente un objeto o una persona con intenciones maliciosas dentro del automóvil, pone en riesgo la computadora de a bordo del vehículo en donde el criminal puede desactivar los frenos mientras se enciende el sistema de limpiaparabrisas en una curva, etc [11].

- En el 2017, se descubrió que decenas de millones de dispositivos como cámaras de vigilancia de aeropuertos, sensores, equipos de red y dispositivos de IoT eran vulnerables debido a una falla que permitía a los cibercriminales obtener control remoto sobre los dispositivos o bloquearlos. La vulnerabilidad encontrada la nombraron "Devil's Ivy". Esta fue descubierto debido a que investigadores de Senrio quienes seleccionaron cámaras de seguridad de alta gama fabricadas por Axis Communications en donde 249 de los 251 cámaras eran vulnerables a atacantes remotos no autenticados que podían interpretar una transmisión de vídeo, reiniciar cámaras o pausar una transmisión de vídeo mientras cometen un delito [12]. Encontraron que no solamente Axis Communications usaba este software defectuoso si no que otras 34 compañías como Microsoft, IBM, Xerox y Adobe.

5. Estado del arte

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]

Tabla 2: Listado de microcontroladores factibles

6. Recursos disponibles

La organización socio formadora ha estipulado que el auditor propuesto no puede superar un costo total de 100 USD; sin embargo ha manifestado su preferencia por un auditor que tenga un costo alrededor de los 50 USD. Para emular dichos dispositivos se propone el uso de dos tarjetas de microprocesador Raspberry Pi 3B (modelo a determinar en base a disponibilidad del laboratorio de robótica).

Para la emulación del centro de control se propone utilizar una instancia de EC2 de Amazon Web Services, en la que se emulará un servidor con una base de datos que utilice MySQL.

7. Objetivos

Los objetivos de este proyecto deben de ser vistos desde 2 esquemas cualitativos:

1. **Fines académicos**: Desarrollo de una primitiva criptográfica de clave pública sin hacer uso de bibliotecas de terceros para el cómputo de las claves. Aclarando que no existen limitaciones para el uso de bibliotecas que realicen de forma eficiente algunas operaciones matemáticas necesarias

2. **Términos ingenieriles**: Desarrollo de una arquitectura de red que permita que un conjunto de dispositivos auditores envíen lecturas de consumo y generación de energía eléctrica a un centro de control por medio de una conexión WiFi. Se parte de que los auditores tienen poder computacional bajo, y los datos generados deben de ser enviados y almacenados de forma segura.

En términos cuantitativos se plantean las siguientes metas:

1. Costo total del dispositivo auditor menor a **100 USD** por pieza.

2. El tiempo de envío seguro de datos debe de ser menor a **15 minutos**, puesto que las lecturas son generadas en ventanas de tiempo de 15 minutos.

8. Arquitectura de red propuesta

Hablar más a detalle de la arquitectura propuesta, enunciando qué componente fungirá cada papel, es como lo que el profe dice de "ponerle nombre y apellido", proponer una nomenclatura para generar identificadores únicos?

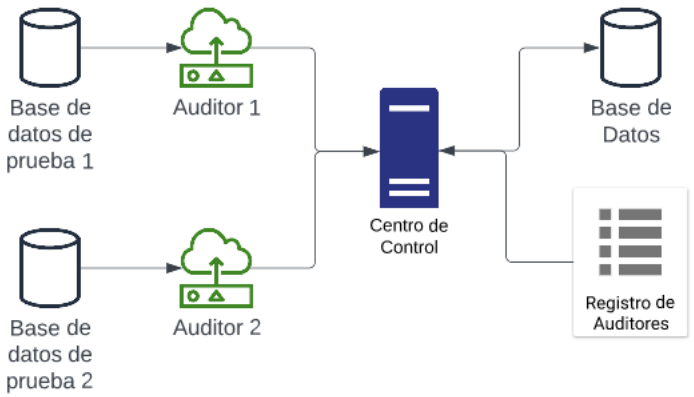

Figura 3: Esquema de arquitectura propuesta

8.1. Sumario de componentes

9. Medio de contacto

El desarrollo del proyecto así como la redacción del presente documento es un trabajo conjunto de:

- Juan Pablo Echeagaray González
- Ricardo Camacho Castillo
- Michelle Yareni Morales Ramóz
- Emily Rebeca Méndez Cruz
- Daniela García Coindreau
- Carolina Longoria Lozano

Así mismo se destacan los siguientes profesores, como asesores y supervisores de los avances en el desarrollo del proyecto:

- Dr. Alberto F. Martínez

Nombre	Manufactura	Arranque	Producción
Auditor 1	▪ Carga de función hash ▪ Contraseña pseudo-aleatoria ▪ Parámetro secreto s ▪ Instalación de software base	▪ Registro de Smart Meters (esquema similar) * ▪ Generación de datagrama de identificación ▪ Envío de datos de identificación a Centro de Control	▪ Recepción de datos de Smart Meters (lectura de datos de prueba) ▪ Encriptado con curva elíptica del datagrama del SmartMeter ▪ Pseudo-firma con función hash escogida por Centro de Control
Auditor 2	▪ Carga de función hash ▪ Contraseña pseudo-aleatoria ▪ Parámetro secreto s ▪ Instalación de software base	▪ Registro de Smart Meters (esquema similar) * ▪ Generación de datagrama de identificación ▪ Envío de datos de identificación a Centro de Control	▪ Recepción de datos de Smart Meters (lectura de datos de prueba) ▪ Encriptado con curva elíptica del datagrama del SmartMeter ▪ Pseudo-firma con función hash escogida por Centro de Control
Centro de Control	Adquisición de instancia de EC2	▪ Selección de parámetros de curva elíptica ▪ Selección de función hash segura contra colisiones ▪ Asignación de hash de identidad para cada auditor	▪ Recepción a los datos publicados por el auditor ▪ Autenticación de la identidad del auditor ▪ Desencriptado y preprocesamiento del datagrama recibido ▪ Envío de actualizaciones de software al auditor para CI/CD ▪ Validación física de los datos recibidos *
Base de Datos	No aplica	Inicialización de esquema de base de datos (predefinido)	▪ Procesado de datos recibidos por el centro de control ▪ Respaldo de datos en la base de datos ▪ Encriptado de la base de datos

Tabla 3: Resumen de componentes empleados

- Dr. Daniel Otero Fadul

El benefactor principal del proyecto es la organización *LiCore*, la comunicación con la organización se vio llevada principalmente por el Dr. Iván S. Razo-Zapata.

En caso de encontrar fallas en el código fuente, o que se necesite de una aclaración de la implementación propuesta; se pide que se abra un *issue* en el repositorio en GitHub que puede ser accedido desde la siguiente liga.

Referencias

[1] 2023. [Online]. Available: https://www.upguard.com/blog/biggest-data-breaches-us

[2] "Cocoa." [Online]. Available: https://www.cocoa-ci.org/

[3] "Smart Grids - Analysis - IEA." [Online]. Available: https://www.iea.org/reports/smart-grids

[4] M. Moran, "Infraestructura - desarrollo sostenible," Jun 2020. [Online]. Available: https://www.un.org/sustainabledevelopment/es/infrastructure/

[5] ——, "Ciudades - desarrollo sostenible," Jun 2020. [Online]. Available: https://www.un.org/sustainabledevelopment/es/cities/

[6] ——, "Consumo y producción sostenibles - desarrollo sostenible," Jun 2020. [Online]. Available: https://www.un.org/sustainabledevelopment/es/sustainable-consumption-production/

[7] "Cost of a data breach 2022: A million-dollar race to detect and respond," 2022. [Online]. Available: https://www.ibm.com/reports/data-breach

[8] *The Aftermath of a Data Breach: Consumer Sentiment*, 2014. [Online]. Available: https://www.ponemon.org/local/upload/file/Consumer%20Study%20on%20Aftermath%20of%20a%20Breach%20FINAL%202.pdf

[9] A. Ríos, "México i arriesgan seguridad con mal uso de iot," Jan 2022. [Online]. Available: https://dplnews.com/mexico-i-arriesgan-seguridad-con-mal-uso-de-iot/

[10] A. Husar, "Iot security: 5 cyber-attacks caused by iot security vulnerabilities," Oct 2022. [Online]. Available: https://www.cm-alliance.com/cybersecurity-blog/iot-security-5-cyber-attacks-caused-by-iot-security-vulnerabilities

[11] F. D. Garcia, D. Oswald, T. Kasper, and P. Pavlides, "Lock it and still lose it - on the (in)security of automotive remote keyless entry systems."

[12] T. Spring, "Bad code library triggers devil's ivy vulnerability in millions of iot devices," Jul 2019. [Online]. Available: https://threatpost.com/bad-code-library-triggers-devils-ivy-vulnerability-in-millions-of-iot-devices/126913/

[13] 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.

[14] 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.

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