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 son una parte esencial del proceso. 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 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 de el auditor a un centro de control. Estos datos son sumamente sensibles, por lo que implementaremos criptografía de clave pública para proteger el almacenamiento y la comunicación de estos datos en el IoT.

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 una arquitectura de clave pública para un *SmartGrid*, que es equivalente a una red heterogénea de dispositivos IoT [2].

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.

3. Planteamiento del problema

Descripción detallada de la situación problema como la presentada en canvas, aquí podemos aprovechar para mostrar diagramas y delimitar el objeto de estudio

4. Justificación

5. Estado del arte

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 tarjeta de microprocesador Raspberry Pi (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?

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