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

1. Introducción **2**

2. Objeto de estudio **2**

3. Planteamiento del problema **2**

4. Justificación **2**

5. Estado del arte **2**

6. Recursos disponibles **3**

7. Objetivos **3**

8. Arquitectura de red propuesta **3**

9. Propuesta metodológica **4**

10. Experimentación y resultados **4**

11. Discusión de resultados **4**

12. Objetivos de Desarrollo Sostenible **4**

13. Medio de contacto **4**

Índice de figuras

Índice de cuadros

1. Introducción

- Descripción general del trabajo que se realizará, mencionando brevemente el caso de negocio que buscamos resolver
- Describir la estructura del reporte técnico

2. Objeto de estudio

Implementación de (protocolo?) criptográfico para el envío de mediciones de generación y consumo de un panel solar a un centro de control por medio de una conexión WiFi. El centro de control para nuestro caso de estudio es una instancia de servidor de EC2 de Amazon, y el conjunto de auditores que procesan y envían esos datos son dispositivos IoT de bajo poder de procesamiento pero costo reducido, suponemos también un uso menor de energía eléctrica

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

Justificar por qué nos deberían de dar recursos para el reto

Descripción de algunos ataques a dispositivos IoT por el mal uso de primitivas criptográficas, creo que no necesita estar específicamente aplicado al caso de estudio de dispositivos de medición de paneles solares, pero si encontramos algún caso, le daría mucha validez al reto, desde aquí le podríamos meter miedo al socio formador

Justificar los requerimientos base del problema (como los que vienen en canvas de criptografía ligera)

5. Estado del arte

Hablar de arquitecturas de red utilizadas en un contexto similar al del reto, ya tenemos algo de P2P, pero tiene que ser algo resumido que después podamos usar para argumentar la selección de red, al final siempre queremos la más sencilla, robusta y económica.

Hablar también de criptografía de clave pública, necesitamos de esta parte principalmente de casos de estudio en los que se hayan aplicado algunas técnicas como RSA/ECC para la generación de las claves privadas y públicas

[NOTE] A partir de aquí somos libres de usar las librerías que queramos

Después debemos de buscar el cómo se hace regularmente el envío de información de un dispositivo IoT hacia un servidor. ¿Hay alguna forma eficiente de realizarlo con alguna librería ya implementada?

Luego debemos de hacer mención de la parte de CI/CD, qué políticas se establecerán para la actualización del software del auditor? Así como las prácticas criptográficas necesarias para validar el software que se descargue

Hablar también de algunas técnicas generales de encriptado de bases de datos, en teoría dispondremos de una instancia de EC2 en la que nosotros tendremos que levantar el servidor y hostear la base de datos

6. Recursos disponibles

Mencionar que tenemos de cota superior 100 dólares, pero que el socio formador prefiere un costo de alrededor de los 50 dólares

Disponemos de acceso a los servicios de EC2 de Amazon para el despliegue de un servidor que podamos usar para hostear una base de datos

7. Objetivos

En fines académicos se busca:

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 que necesitemos

En términos ingenieriles:

Desarrollo de un sistema de monitoreo de consumo y producción eléctrica de una vivienda, dicho sistema enviará cada determinado lapso de tiempo las lecturas pertinentes a un centro de control por medio de una conexión a internet. Se busca también que dicha información se almacene dentro de una base de datos para su análisis futuro.

Las etapas anteriormente mencionadas

De forma concreta en términos económicos y de tiempo computacional:

Se busca que el auditor propuesto tenga un costo inferior a los 100 USD, pero que de preferencia se encuentre en un precio menor a 50 USD

El envío de las lecturas debe de ocurrir cada 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. Propuesta metodológica

Enunciar los pasos del reto en el orden correcto [TEMP] Necesito validar con el profe que estos sean los correctos: Arranque de la red

10. Experimentación y resultados

Generar un análisis estadístico sencillo del tiempo de cómputo de nuestra implementación, podemos compararla con el de librerías prestablecidas

Demostrar que nuestra implementación cumple con una suite de vectores de prueba, que puede estar basada en los de las librerías grandes

11. Discusión de resultados

En esta parte argumentamos la eficiencia de nuestra implementación con los datos de la sección pasada

12. Objetivos de Desarrollo Sostenible

Argumentar el por qué se han seguido los 3 ODS propuestos en canvas:

Objetivo 7. Garantizar el acceso a una energía asequible, segura, sostenible y moderna para todos.

Objetivo 9. Industria, innovación e infraestructura (ej. Protección de entornos Wireless, Navegación segura por Internet, entornos Near Field Communication (NFC)).

Objetivo 13. Adoptar medidas urgentes para combatir el cambio climático y sus efectos.

13. 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 Coindreaz
- 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