Prototipo de sistema de cifrado de información basado en algoritmos de cifrado ligero y hardware dedicado para aplicaciones de Internet de las Cosas

Trabajo Terminal No. 2020 – A066

*Alumnos: Camacho Reyes Brandon Israel 1, *Sabas Hernández José Rodolfo 2*
Directores: García Ortega Víctor Hugo 1, Cortez Duarte Nidia Asunción 2
**e-mail: joserodolfosabashernandez@gmail.com*

Resumen – El presente trabajo terminal tiene como objetivo el desarrollo de un sistema de cifrado de la información de un nodo sensor ante la necesidad de brindar seguridad a estos datos sensibles al viajar a través de internet. Por un lado, se implementará un algoritmo de cifrado ligero en un microcontrolador; por otro lado, se hará la configuración de un Core de cifrado en hardware en un microcontrolador.

Palabras clave – Sistema embebido, microcontroladores, criptografía ligera, criptografía en hardware.

1. Introducción

Una microrred (microgrid) es una interfaz que permite la conexión de una fuente de energía renovable con la red eléctrica, así como el suministro de cargas directamente. Algo importante, es la flexibilidad y autonomía que proporcionan ya que en caso de fallas en la red de distribución pueden proporcionar energía directamente al usuario. A este nuevo esquema de generación de energía se le conoce como Generación Distribuida (DG-Distributed Generation). [1]

Para realizar el monitoreo de microrredes se utiliza una red inalámbrica de sensores (WSN-Wireless Sensor Network), esta red está formada por nodos sensores autónomos.[1]

Los nodos sensores son un sistema computacional de software y hardware diseñados para realizar tareas específicas y son usados para monitorear de forma autónoma (sin intervención humana) diferentes parámetros de una microrred para determinar su estado en cualquier momento dado, están encargados de recopilar información sensible del mundo físico y transmitirla hacia otros nodos conectados en la red. Además, nos proporcionan ventajas de rendimiento, costo y usabilidad, y son denominado un sistema embebido.[1]

En muchas aplicaciones los nodos sensores necesitan enviar los datos obtenidos hacia un servidor remoto a través de internet, por lo que se usa el concepto de Internet de las Cosas (IoT-Internet of Things).

Debido a que la información viaja a través de internet, y siendo este un canal inseguro, se necesita de mecanismos de cifrado para brindar ciertos servicios de seguridad.

La mayoría de los estándares en criptografía son costosos computacionalmente por lo que no se recomiendan para IoT, sin embargo, existen alternativas como son algoritmos de criptografía ligera y criptografía en hardware**.**

La infraestructura de clave pública no es adecuada para entornos de IoT, ya que se convierte en una tarea computacionalmente costosa calcular el texto cifrado debido al gran tamaño de la clave.

La criptografía ligera se centra en nuevos diseños, adaptaciones o implementaciones eficientes de primitivas y protocolos criptográficos con una complejidad de implementación muy baja. Debido a las severas restricciones de costos, es decir, en recursos de hardware. [2]

Actualmente para poder agregar seguridad a procesadores con bajos recursos (microcontroladores) se puede usar alguna de estas opciones:

1. Se puede programar el algoritmo de cifrado completo usando el conjunto de instrucciones que proporciona el procesador (lenguaje ensamblador, lenguaje C).
2. Seleccionar un microcontrolador que contenga una unidad de cifrado como un periférico incorporado, el cual tiene que ser configurado usando su conjunto de instrucciones.
3. Utilizar un core de cifrado implementado en un SoC (System on Chip) de forma externa al microcontrolador, este SoC se comunica mediante una interfaz serial (UART, SPI).
4. Utilizar un core de cifrado implementado en un SoPC (System on Programmable Chip – FPGA) de forma externa al microcontrolador, este SoPC se comunica mediante una interfaz serial.

En este trabajo terminal se propone implementar un algoritmo de cifrado ligero usando las opciones 1 y 2.

Algunos trabajos similares de la literatura abierta se describen a continuación.

Gaurav Bansod, en [3], presenta el diseño de un sistema de cifrado compacto y liviano basado en la operación del grupo de instrucción de permutación de bits (GRP), usando el cuadro S de PRESENT, agregando la propiedad de confusión para GRP, implementado en el procesador LPC2129 de 32 bits.

Gandu Ramu, en [4], propone la implementación en hardware del algoritmo de cifrado ligero PICCOLO con una llave de 80 bits, donde su arquitectura de hardware propuesta utiliza 75 flip-flops, 282 slices y 132.25MHz de frecuencia de un dispositivo FPGA Spartan3an y 72 flip-flops, 194 slices y una frecuencia de 280.94MHz en un dispositivo FPGA Virtex-5.

William Diehl, en [5], realiza la implementación y comparación en hardware y software con la métrica (TP/A) de los algoritmos de cifrado ligero SIMON, SPECK, PRESENT, LED, TWINE), así como AES, en un FPGA Kintex-7 de 8 bits reconfigurable con un objetivo de área de 300-400 LUT. Obtuvieron como resultado que AES ocupa un lugar alto en la implementación en software pero bajo en hardware y SIMON ocupa un lugar alto en hardware y bajo en software.

2. Objetivo

Implementar un prototipo de un sistema de cifrado de la información recolectada en un nodo sensor usando algoritmos de cifrado ligero y hardware de propósito específico para agregar seguridad en aplicaciones de Internet de las Cosas.

Objetivos Específicos

- Analizar y seleccionar un algoritmo de cifrado ligero.
- Implementar el algoritmo de cifrado ligero en un microcontrolador haciendo uso de su conjunto de instrucciones (lenguaje ensamblador y lenguaje C).
- Implementar el proceso de descifrado para el algoritmo de cifrado ligero en la computadora (haciendo uso de bibliotecas criptográficas existentes).

- Analizar y seleccionar un microcontrolador que cuente con un core dedicado de criptografía como un periférico.

- Implementar el programa para la configuración del core dedicado de criptografía en el microcontrolador.

- Implementar el proceso de descifrado para el algoritmo que tiene implementado el core dedicado en la computadora (haciendo uso de bibliotecas criptográficas existentes).

3. Justificación

El problema de seguridad que afecta el paradigma de IoT ha atraído recientemente una atención significativa de la comunidad de investigación.

Los dispositivos IoT implantables y portátiles monitorean y extraen mediciones vitales para permitir alertas de emergencia en tiempo real, por ejemplo, los sensores IoT desplegados en las fábricas controlan la contaminación ambiental y las fugas químicas en el suministro de agua, mientras que los sensores de humo, gases tóxicos y temperatura junto con los sistemas de advertencia previenen los desastres ecológicos.[6]

De hecho, varios estudios del caso han informado sobre el impacto significativo de IoT en la integridad y el consumo de los recursos naturales. Por ejemplo, los sensores de presión de agua en las tuberías monitorean la actividad del flujo, estos datos pueden ser recibidos por un nodo sensor y posteriormente notificados a los operadores, por ejemplo, en caso de una fuga.[6]

Dado a que la información que llega y se transmite en este nodo sensor es sensible, los datos tienen que llegar a su destino con integridad, sin que un adversario haya obtenido o alterado la información de dichos datos en el medio, ya que una alteración en esta, podría causar que se transmitan resultados falsos. Es por ello que la seguridad de la información en una red de nodos sensores es de gran importancia.

Las soluciones de IoT centradas en la seguridad se esfuerzan por minimizar los escenarios y situaciones peligrosas.[6]

Varias dificultades técnicas, que incluyen capacidades limitadas de almacenamiento, energía y cómputo, desafían abordar varios requisitos de seguridad de IoT. Por ello es necesario implementar mecanismos de seguridad de bajo costo computacional.

La criptografía ligera es un campo interesante que logra el equilibrio perfecto para proporcionar seguridad, mayor rendimiento, bajo consumo de energía, compacidad y sobre todo una mayor portabilidad.[3]

Por su parte, los algoritmos de cifrado en hardware nos proporcionan una mayor rapidez y eficiencia, sin embargo, estos no están disponibles en todos los modelos de microcontroladores.

4. Productos o Resultados esperados

El prototipo de sistema propuesto tiene como objetivo cifrar la información que recibe un “nodo sensor” con la finalidad de brindar mayor seguridad a esa información sensible al viajar a través de internet.

La arquitectura general del sistema se muestra en la Figura 1. El sistema propuesto es parte de un sistema de monitoreo de parámetros aplicados a una microrred eléctrica que utiliza un panel solar como fuente de energía renovable. En la sección marcada con el recuadro continuo en rojo se aplicarán los algoritmos de cifrado a desarrollar en esta propuesta y los algoritmos de descifrado se implementarán del lado del servidor.

Cabe mencionar que no se utilizará el panel solar físico ni el sensor, en su lugar se usará una arquitectura de prueba para los algoritmos propuestos.

La arquitectura del sistema de cifrado se muestra en la Figura 2 por medio de diagramas de bloques.

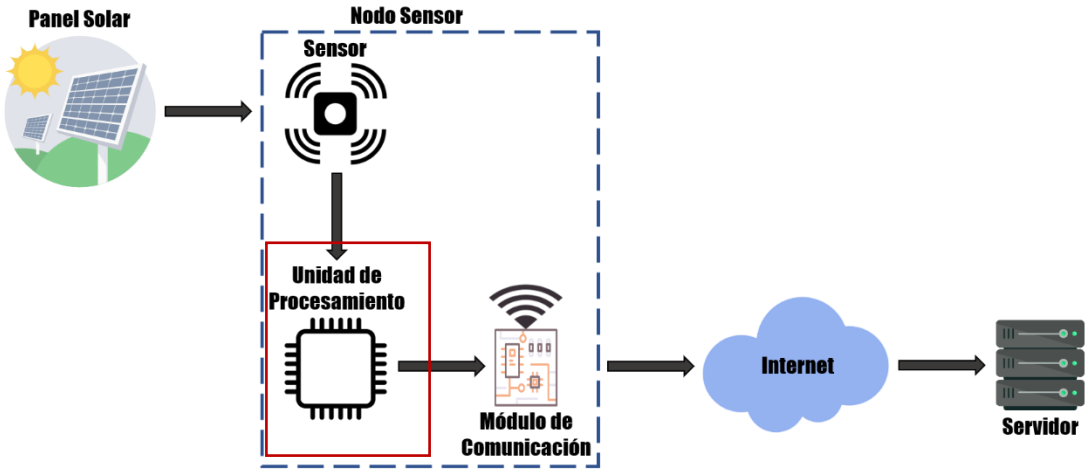

Figura 1. Arquitectura general del sistema. Fuente: Creación propia

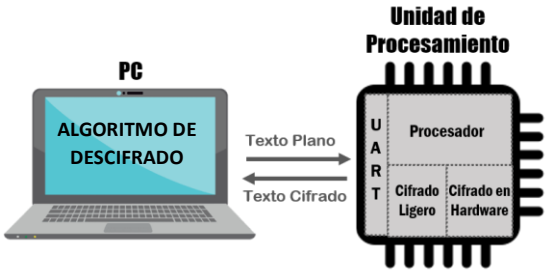

Figura 2. Arquitectura del sistema de cifrado. Fuente: Creación propia

En este trabajo terminal se desarrollarán las siguientes dos actividades:

- Implementar un algoritmo de cifrado ligero usando el conjunto de instrucciones que proporciona el procesador (lenguaje ensamblador, lenguaje C). Las pruebas se realizarán cifrando datos en el microcontrolador y descifrándolos en la PC.
- Implementar el programa de configuración de un microcontrolador que cuente con un core dedicado para el cifrado usando el lenguaje ensamblador y C. Las pruebas se realizarán cifrando datos en el microcontrolador y descifrándolos en la PC.

Al finalizar el presente trabajo, se espera contar con los siguientes productos:

- Implementación de un algoritmo de cifrado ligero en un microcontrolador
- Configuración de un Core de cifrado en hardware en un microcontrolador
- Manual técnico del sistema
- Artículo de divulgación científica
- Pruebas al sistema con datos enviados por una computadora

5. Metodología

Para la implementación de este prototipo se tomó en cuenta una adaptación del modelo en V para el desarrollo de sistemas embebidos, la cual consta de 7 etapas, en las cuales se parte de un análisis y diseño, siguiendo una implementación y por último una depuración e integración final. Las etapas que tiene este modelo se muestran en la Figura 3.

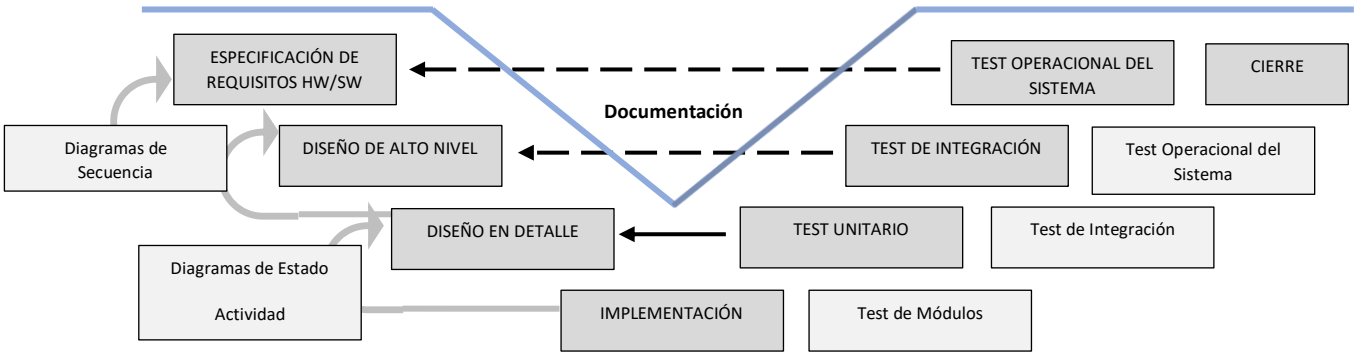

Figura 3. Modelo en V

A continuación, se detalla de forma general cada etapa:

- Especificación de requisitos HW/SW: Se pretende definir y documentar los diferentes requerimientos del sistema a implementar como: Los servicios criptográficos requeridos en la problemática, el microcontrolador con Core dedicado a utilizar, así como los recursos de hardware disponibles.
- Diseño de alto nivel: El cual tiene como objetivo obtener una visión general del sistema.
- Diseño en detalle: Consiste en detallar cada bloque de la fase anterior, aquí se pretende especificar el diseño del algoritmo de cifrado ligero en software, así como la configuración necesaria para el uso del Core dedicado del microcontrolador y se especifica el diseño del algoritmo de descifrado en la PC.
- Implementación: En esta etapa se implementa cada módulo de la etapa anterior.

- Test Unitario: Verifica cada módulo de HW y SW de manera individual, en donde se depurará cada uno de los módulos hasta obtener el resultado deseado.
- Test de Integración: Acopla los diferentes módulos del sistema.
- Test Operacional: Se realizan las últimas pruebas sobre un escenario real.

6. Cronograma

Los cronogramas por integrante se muestran anexos a este documento

7. Referencias

[1] V.H. Garcia, R. Ortega, R.J. Romero. "Embedded system for the communication and monitoring of an electric microgrid using IoT" pp.13

[2] B. Preneel, Understanding Cryptography. London New York. Springer Verlag. 2010

[3] Bans, G., Raval, N., and Pisharoty, N.(2015) Implementation of a New Lightweight Encryption Design for Embedded Security. IEE, 10(1), pp.1.

[4] Gandu, R., Zeesha, M. and Acharya,B.,(2019) Hardware implementation of Piccolo Encryption Algorithm for constrained RFID application. IEEE, pp.88.

[5] William, D., Farnoud F., Panasayya Y, Kaps J. and Gaj, K., (2017). Comparison of Hardware and Software Implementations of Selected Lightweight Block Ciphers. IEEE, 1-4.

[6] Neshenko, N., Bou-Harb., L., Crichigno, J., Kaddoum, G., Ghani, N. (2019). Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations. *IEEE, 21*(3), pp.32.

[7] PEREZ, A; et al. "Una metodología para el desarrollo de hardware y software embebidos en sistemas críticos de seguridad". Systemics, Cybernetics and Informatics Journal, vol 3, Num. 2, 2006, pp. 70-75.

8. Alumnos y Directores

Camacho Reyes Brandon Israel.- Alumno de la carrera de Ing. en Sistemas Computacionales en ESCOM, Especialidad en Sistemas, Boleta: 2015010140, Tel. 5510688376, email. brandon.6.1.9@hotmail.com

Sabas Hernández José Rodolfo.- Alumno de la carrera de Ing. en Sistemas Computacionales en ESCOM, Especialidad en Sistemas, Boleta: 2015090687, Tel. 5574440836, email. joserodolfosabashernandez@gmail.com

García Ortega Victor Hugo.- Ing. en Sistemas Computacionales egresado de la Escuela Superior de Cómputo del Instituto Politécnico Nacional (IPN-1999). Maestría en Ingeniería de Cómputo con especialidad en Sistemas Digitales en el Centro de Investigación en Computación del IPN (2006). Actualmente es profesor Titular en la Escuela Superior de Cómputo del IPN trabajando en el área de Sistemas embebidos, Arquitectura de Computadoras y Procesamiento Digital de Imágenes y Señales.

Cortez Duarte Nidia Asunción.- Maestra en Ciencias en Computación CINVESTAV-IPN 2009, Ing. en Sistemas Computacionales ESCOM-IPN 2006, Profesora en ESCOM Depto. de Ingeniería en Sistemas Computacionales. Áreas de interés: criptografía, seguridad de información, hardware reconfigurable, aritmética computacional, redes de computadoras

Cronogramas

Nombre del alumno(a): Camacho Reyes Brandon Israel TT No.: 2020 - A066
Título del TT: Prototipo de sistema de cifrado de información basado en algoritmos de cifrado ligero y hardware dedicado para aplicaciones de Internet de las Cosas

Actividad	AGO	SEP	OCT	NOV	DIC	ENE	FEB	MAR	ABR	MAY	JUN
Especificación de requisitos de algoritmo de cifrado en hardware dedicado											
Análisis y selección de algoritmo de cifrado en hardware dedicado											
Diseño de Alto Nivel del algoritmo para el cifrado en hardware dedicado											
Diseño en detalle de algoritmo de cifrado en hardware dedicado											
Presentación											
Implementación del programa para el cifrado en hardware dedicado											
Test unitario de algoritmo de cifrado en hardware dedicado											
Test de integración de algoritmo de cifrado en hardware dedicado											
Test operacional del sistema de algoritmo de cifrado en hardware dedicado y descifrado en la computadora.											
Presentación											
Elaboración del Documento											

Nombre del alumno(a): Sabas Hernández José Rodolfo TT No.: 2020 - A066

Título del TT: Prototipo de sistema de cifrado de información basado en algoritmos de cifrado ligero y hardware dedicado para aplicaciones de Internet de las Cosas

Actividad	AGO	SEP	OCT	NOV	DIC	ENE	FEB	MAR	ABR	MAY	JUN
Especificación de requisitos de hardware software de algoritmo de cifrado ligero											
Análisis y selección de algoritmo de cifrado ligero											
Diseño de Alto Nivel de algoritmo de cifrado ligero											
Diseño en detalle de algoritmo de cifrado ligero											
Presentación											
Implementación de algoritmo de cifrado ligero											
Test unitario de algoritmo de cifrado ligero											
Test de integración de algoritmo de cifrado ligero											
Test operacional del sistema de algoritmo de cifrado ligero y descifrado en la computadora											
Presentación											
Elaboración del Documento											

Gmail **Brandon Camacho Reyes <lestat150415@gmail.com>**

CD Protocolo Final TT#2020-A066

Nidia A. Cortez <nidiacortez3@gmail.com> 18 de agosto de 2021, 23:42
Para: Brandon Camacho Reyes <lestat150415@gmail.com>

Buenas noches por medio de este correo notifico que estoy de acuerdo con la versión final del Protocolo de TT 2020 A066 titulado Prototipo de sistema de cifrado de información basado en algoritmos de cifrado ligero y hardware dedicado para aplicaciones de Internet de las cosas.

El protocolo ha sido integrado al CD que los alumnos Brandon y José entregarán a la CATT.

M. en C. Nidia Asunción Cortez Duarte
Directora del TT 2020 A066
[Texto citado oculto]
--
Nidia A. Cortez Duarte
Profesor Titular B
Escuela Superior de Cómputo IPN
Tel. 57 29 6000 ext. 52032

Gmail **Brandon Camacho Reyes <lestat150415@gmail.com>**

CD Protocolo Final TT#2020-A066

Victor Garcia <vgarciaortega@yahoo.com.mx> 4 de septiembre de 2021, 11:36
Para: Brandon Camacho Reyes <lestat150415@gmail.com>

"Buenas noches por medio de este correo notifico que estoy de acuerdo con la versión final del Protocolo de TT 2020 A066 titulado Prototipo de sistema de cifrado de información basado en algoritmos de cifrado ligero y hardware dedicado para aplicaciones de Internet de las cosas.

El protocolo ha sido integrado al CD que los alumnos Brandon Israel Camacho Reyes y José Rodolfo Sabas Hernandez entregarán a la CATT."

M. en C. Victor Hugo Garcia Ortega
Instituto Politécnico Nacional
Escuela Superior de Cómputo
Departamento de Ingeniería en Sistemas Computacionales
Academia de Sistemas Digitales
Tel. (52)55 57296000 ext. 52064