Securing Data in Low-Resource Systems: Lightweight Block Cryptography Strategies

Fernando Ramirez Arredondo
dept. name of organization (of Aff.)
name of organization (of Aff.)
Arequipa, Perú
fernando.ramirez@ucsp.edu.pe

Yván Jesús Túpac Valdivia
dept. name of organization (of Aff.)
name of organization (of Aff.)
Arequipa, Perú
ytupac@ucsp.edu.pe

***Abstract*—Aquí deberá colocar el abstract del trabajo en español. No debe modificar el formato de este documento, decir, no debe cambiar ni el tipo ni el tamaño de la fuente. No debe cambiar el ancho de los márgenes. No debe cambiar el interlineado, etc.**

***Index Terms*—IoT, Feistel, Substitution-Permutation**

I. Introducción

Aquí deberá colocar la introducción del paper. Debe incluir un contexto (situar el tema), la descripción de un problema, el objetivo y la organización del texto. Esta sección no debe tener subsecciones. La descripción debe seguir la descripción en embudo, es decir de los más general a lo más específico.

En 2016, el fundador y presidente ejecutivo del Foro Económico Mundial, Klaus Schwab, publicó un libro titulado La Cuarta Revolución Industrial, en el cual explicaba que la forma en que vivimos, trabajamos y nos relacionamos unos con otros estaba a punto de ser alterada fundamentalmente por una revolución digital diferente a las que la humanidad había experimentado antes. Volviendo al día de hoy, esta llamada cuarta revolución industrial se ha caracterizado por una fusión de tecnologías que está difuminando las fronteras entre las esferas física, digital y biológica [1].

El paradigma del Internet de las cosas (IoT, por sus siglas en inglés) corresponde al campo creado por dispositivos integrados con electrónica, software, sensores y conectividad, lo que permite la transmisión, recepción y procesamiento de datos a través de diversas infraestructuras de comunicación. El IoT genera más oportunidades para la integración directa entre el mundo físico y los sistemas basados en computadora.

Hasta el año 2019, el IoT, que solía operar en espacios de redes más pequeños, se ha expandido a redes de área amplia, aumentando así los riesgos asociados debido al esperado aumento en dispositivos IoT en diversos entornos. Con el rápido crecimiento de las aplicaciones de IoT, se genera y se intercambia una cantidad sustancial de datos sensibles, lo que ha llevado a la observación de varios problemas de seguridad y privacidad. A medida que los dispositivos se vuelven más interconectados, las preocupaciones de seguridad y privacidad se volverán más pronunciadas, exponiendo continuamente fallas y debilidades de seguridad adicionales. En términos estadísticos, todos los errores y debilidades expuestos pueden ser explotados en un entorno con miles de millones de dispositivos.

Thakor et al. categorizaron los dispositivos IoT en dos grupos según sus recursos [2]. El primer grupo incluye dispositivos abundantes en recursos como servidores, computadoras personales, tabletas, teléfonos inteligentes, etc. El segundo grupo comprende dispositivos limitados en recursos, como sensores industriales o nodos de sensores, etiquetas RFID, actuadores, etc.

Este último grupo de dispositivos enfrenta múltiples restricciones, incluidas limitaciones en recursos, memoria, consumo de energía y velocidad. El desafío en términos de rendimiento surge al intentar implementar criptografía tradicional en dispositivos con recursos limitados. Esta dificultad se atribuye a las operaciones matemáticas complejas y exigentes en recursos involucradas en técnicas criptográficas tradicionales, que requieren un espacio de memoria sustancial y una alta potencia de procesamiento. El costo de implementación de la criptografía tradicional en dispositivos de baja capacidad de recursos es notablemente alto. En consecuencia, se introdujo la criptografía ligera, surgida de la notable expansión en tecnologías ubicuas emergentes, como una técnica criptográfica moderna para abordar estos problemas.

Los cifrados se clasifican como asimétricos o simétricos. Aunque los cifrados asimétricos ofrecen características de seguridad mejoradas, requieren más potencia de cálculo y tienden a ser relativamente más costosos. Debido a estas razones, los cifrados asimétricos no son tan populares en dispositivos con recursos limitados. Dentro de las dos principales clasificaciones de cifrados simétricos, los cifrados por bloques y por flujo son los más destacados. Este estudio se enfoca en los cifrados por bloques, concretamente detallando las estructuras de la Red de Sustitución-Permutación (Substitution-Permutation Network) [3] y la Red de Feistel (Feistel Network) [4], que se encuentran en la sección III. Luego, en la sección IV, se presentarán los resultados de los experimentos realizados.

II. Estado del Arte

Aquí deberá colocar el estado del arte de la investigación.

En el estudio de Fan et al. [5], se definió un cifrado ligero como un algoritmo criptográfico diseñado específicamente para dispositivos con recursos limitados. El algoritmo necesitaba abordar tres desafíos clave: minimizar la sobrecarga (en términos de área de silicio o huella de memoria), garantizar un bajo consumo de energía y mantener un nivel suficiente de seguridad.

Otros investigadores han adoptado un enfoque cuantitativo para la definición de cifrados ligeros. Por ejemplo, en el estudio realizado por Cazorla et al. [6] se propusieron criterios específicos para categorizar un cifrado como ligero. Estos criterios abarcan atributos como el tamaño del bloque, el tamaño de la clave, las operaciones y la programación de claves. En el contexto de los cifrados de bloque ligeros, el término "ligero" denota un tamaño de bloque reducido (32, 48 o 64 bits) en contraste con los cifrados convencionales, que suelen tener tamaños de bloque más grandes (64 o 128 bits).

El informe NIST IR 8114 [7], trabajando hacia la estandarización de estos algoritmos, define la criptografía ligera como un subcampo de la criptografía que tiene como objetivo proporcionar soluciones adaptadas para dispositivos con recursos limitados.

En los últimos años, se han generado notables avances en los cifrados de bloques ligeros, con varias contribuciones importantes que han mejorado tanto la eficiencia como la seguridad. IVLBC, presentado por Huang et al. [8] en 2022, se caracterizó por su tamaño de bloque de 64 bits y longitudes de clave de 80 y 128 bits, junto con 29 rondas de iteración. Al utilizar S-boxes involutivas livianas y permutaciones basadas en nibble, IVLBC permitió la reutilización de circuitos y códigos entre cifrado y descifrado.

DULBC, propuesto también en 2022 por Yang et al. [9], ofreció un cifrado ligero y dinámico con un tamaño de bloque de 64 bits y longitudes de clave de 80 y 128 bits. Este algoritmo empleó funciones redondas dependientes de claves y demostró una superioridad en la complejidad del criptoanálisis exponencial sobre las alternativas estáticas.

LBCCS, propuesto en el mismo año por Zhu et al. [10], ofrecía 20 rondas con bloques y claves de 128 bits. Este algoritmo construyó S-boxes altamente seguras y P-boxes difusivas utilizando sistemas caóticos combinacionales, a la vez que reducía la complejidad mediante una función de ronda adaptable. Sin embargo, la implementación en hardware de LBCCS requería un costo considerable, llegando a alcanzar los 2227 GE, lo que resalta los desafíos inherentes en la búsqueda de eficiencia, a pesar de las sofisticadas características criptográficas que presenta.

SCENERY, introducido también en 2022 por Feng y Li [11], se caracterizaba por su tamaño de bloque y clave de 64 y 80 bits respectivamente, con 28 rondas. Mediante su función de ronda que constaba de 8 S-boxes paralelas de 4×4 y una matriz de difusión binaria de 32×32, SCENERY demostró una eficiencia notable en requisitos de hardware, con un total de 1438 GE, posicionándose por debajo de otros algoritmos de cifrado comparables.

En 2021, LBC-IoT surgió como un cifrado ultraligero propuesto por Ramadan et al. [12], con un tamaño de bloque de 32 bits, una longitud de clave de 80 bits y 32 rondas. LBC-IoT minimizó los costos de hardware mediante la utilización de S-boxes, desplazamientos laterales y XOR de 4 bits, lo que requirió solo 548 GE en hardware.

III. Técnicas para resolver el problema

Aquí deberá dar la descripción detallada de las técnicas que va a comparar y que por lo tanto va a implementar. Deberá crear dos secciones, una para cada técnica.

A. Substitution-Permutation Network

B. Feistel Network

IV. Experimentos y Resultados

En esta sección debe colocar los experimientos y resultados. Si el proyecto todavía no tiene resultados, debe eliminar esta sección.

V. Conclusiones

Aquí debe colocar las conclusiones

References

[1] "World Economic Forum the fourth industrial revolution: what it means, how to respond," https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/, accessed: 2023-11-07.

[2] V. Thakor, M. A. Razzaque, and M. Khandaker, "Lightweight cryptography algorithms for resource-constrained iot devices: A review, comparison and research opportunities," *IEEE Access*, vol. 9, pp. 28 177–28 193, 01 2021.

[3] H. M. Heys and S. E. Tavares, "Substitution-permutation networks resistant to differential and linear cryptanalysis," *Journal of cryptology*, vol. 9, no. 1, pp. 1–19, 1996.

[4] V. Nachef, J. Patarin, and E. Volte, "Feistel ciphers," *Cham: Springer International Publishing*, 2017.

[5] X. Fan, K. Mandal, and G. Gong, "Wg-8: A lightweight stream cipher for resource-constrained smart devices," in *Quality, Reliability, Security and Robustness in Heterogeneous Networks: 9th International Conference, QShine 2013, Greader Noida, India, January 11-12, 2013, Revised Selected Papers 9*. Springer, 2013, pp. 617–632.

[6] M. Cazorla, K. Marquet, and M. Minier, "Survey and benchmark of lightweight block ciphers for wireless sensor networks," in *2013 international conference on security and cryptography (SECRYPT)*. IEEE, 2013, pp. 1–6.

[7] K. McKay, L. Bassham, M. Sönmez Turan, and N. Mouha, "Report on lightweight cryptography," National Institute of Standards and Technology, Tech. Rep., 2016.

[8] X. Huang, L. Li, and J. Yang, "Ivlbc: An involutive lightweight block cipher for internet of things," *IEEE Systems Journal*, 2022.

[9] J. Yang, L. Li, Y. Guo, and X. Huang, "Dulbc: A dynamic ultra-lightweight block cipher with high-throughput," *Integration*, vol. 87, pp. 221–230, 2022.

[10] D. Zhu, X. Tong, Z. Wang, and M. Zhang, "A novel lightweight block encryption algorithm based on combined chaotic system," *Journal of Information Security and Applications*, vol. 69, p. 103289, 2022.

[11] J. Feng and L. Li, "Scenery: a lightweight block cipher based on feistel structure," *Frontiers of Computer Science*, vol. 16, no. 3, p. 163813, 2022.

[12] R. A. Ramadan, B. W. Aboshosha, K. Yadav, I. M. Alseadoon, M. J. Kashout, and M. Elhoseny, "Lbc-iot: Lightweight block cipher for iot constraint devices." *Computers, Materials & Continua*, vol. 67, no. 3, 2021.