UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS

Revista Vínculos

https://revistas.udistrital.edu.co/index.php/vinculos/

A+T Actualidad Tecnológica

Uso del algoritmo AES en las tecnologías de IoT

Use of the AES algorithm in IoT technologies

Brayan Daniel Navarro Ortiz [1], Cristian Nicolás García García [2], Juan Sebastián Buitrago Romero [3]

Para citar este artículo: B. D. Navarro Ortiz, C. N. García García, J. S. Buitrago Romero, "Uso del algoritmo AES en las tecnologías de IoT", Revista Vínculos, vol 19, no. 1, p-p 51-55, 2022. https://doi.org/10.14483/2322939X.17669

Recibido: 12-12-2021 / Aprobado: 07-02-2022

Resumen: Se analiza la implementación del algoritmo AES en dispositivos utilizados en IoT, haciendo énfasis en la seguridad que brinda este algoritmo en dichos dispositivos, de las consecuencias que trae dicha implementación en donde a pesar de los inconvenientes presentados, se generan avances de diversas formas de implementar el algoritmo AES en los microprocesadores.

Palabras clave: IoT, AES, Encriptación, Seguridad, Microcontrolador.

Abstract: In this article, an analysis will be carried out on the implementation of the AES algorithm in devices used in IoT, the security provided by this algorithm in said devices will be analyzed in addition to the consequences that said implementation brings, in addition to said inconveniences, advances are generated in various ways to implement the AES algorithm in the microprocessors.

Keywords: IoT, AES, Encryption, Security, Microcontroller.

1 Tecnólogo en sistematización de datos, Universidad Distrital, Colombia - Bogotá. bdnavarroo@correo.udistrital.edu.co
2 Tecnólogo en sistematización de datos, Universidad Distrital, Colombia - Bogotá. cngarciag@correo.udistrital.edu.co
3 Tecnólogo en sistematización de datos, Universidad Distrital, Colombia - Bogotá. jsbuitragor@correo.udistrital.edu.co

1. Introducción

Con el paso de los años la ingeniería ha observado el aumento continuo de tecnología IoT y a su vez problemas de seguridad de la información a nivel mundial, este crecimiento ha fomentado la búsqueda de soluciones alternativas. La aplicación de medidas de seguridad sólidas para un dispositivo de IoT simple podría parecer un caso de sobre ingeniería, pero incluso los dispositivos simples de sensores de temperatura que carecen de protección suficiente pueden proporcionar a los piratas informáticos un punto de entrada a las redes corporativas. De hecho, la seguridad de la IoT se enfrenta a constantes desafíos debido a la combinación de la conectividad omnipresente que proporcionan las aplicaciones de IoT y los dispositivos de recursos limitados que subyacen a estas aplicaciones. Adicionalmente, incluso en los diseños de dispositivos de IoT con suficientes recursos para ejecutar algoritmos de criptografía en el software y las aplicaciones.

La lección objetiva de esta mirada, ciertamente superficial a estos algoritmos, se basa en una secuencia de operaciones matemáticas diseñadas para que los intentos de comprometer los resultados sean tan costosos desde el punto de vista computacional que es imposible -o inviable- completarlos con la suficiente rapidez como para ser útiles al autor. Además, incluso una inspección superficial de cada algoritmo sugiere que un dispositivo de IoT con recursos limitados, probablemente tendrá pocas posibilidades de ejecutar una implementación de software del algoritmo sin comprometer potencialmente los requisitos funcionales primarios del dispositivo. Por último, los detalles precisos del algoritmo más allá de los pasos que se muestran aquí, significan que incluso un sutil error de codificación o una pequeña mala interpretación de la norma puede dar lugar a vulnerabilidades de seguridad, o incluso a un fallo total del proceso criptográfico. pueden seguir siendo vulnerables debido a sutiles errores en la aplicación de estos algoritmos. En este artículo se explica el uso del algoritmo de encriptación de AES en tecnologías de IoT en relación con seguridad.

2. AES

Estándar de cifrado avanzado (AES) que utiliza arquitecturas multiplexadas en el tiempo para dispositivos de borde. La optimización se lleva a cabo de forma cuádruple en hardware de cifrado / descifrado AES basado en el mecanismo de intercambio de recursos con un cuadro de sustitución modificado que alcanza una frecuencia de funcionamiento máxima de 1.053GHz [1].

La aplicación del algoritmo AES en controladores, garantiza la transmisión de información con un alto grado de confiabilidad a través de cualquier red IP, ya que estos datos al ser vulnerables pueden engañar al sistema y generar caos en las

ISSN 1794-211X • e-ISSN 2322-939X • Vol 19, N° 1 (enero-junio 2022). pp. 51-55. Universidad Distrital Francisco José de Caldas-Facultad Tecnológica.

redes. Es indispensable el estudio de criptografía en dispositivos computacionales, como los microcontroladores en vista de su implementación en redes, debido a la necesidad de asegurar la información que se transmite a través de redes públicas, para reducir riesgos de pérdida y suplantación de información por su captura ilegal.

Por lo general, un microcontrolador que es utilizado para transmitir información a través de una red carece de algún método que proporcione seguridad y confiabilidad en los mensajes enviados, este puede ser uno de los grandes enigmas del uso de dispositivos electrónicos de bajo poder computacional en sistemas de comunicación. Con la aplicación eficaz de un algoritmo criptográfico como AES, se obtiene una solución a bajo costo y confiable para proteger la información [2].

En proyectos que desean implementar el cifrado de información puede ocurrir que, entre el transmisor y el receptor, sea complejo realizar el intercambio o la programación inicial de las claves, por tal razón, las librerías de cifrado AES podrían complementarse con el diseño de un algoritmo criptográfico de clave pública que permita resolver fácil y eficazmente el problema del intercambio inicial de claves.

3. AES en IoT

Es común hablar de seguridad ya que en la actualidad se puede tener toda la información de miles de personas expuestas a personas que quieran robar o dar uso inadecuado, así que el tema de seguridad siempre está presente en cada implementación ya sea de un servicio, producto o componente que haga uso de la información, ahora si se habla de un ambiente IoT donde la información es una base importante de este y la información está presente en múltiples dispositivos viajando de uno a otro, hace que el tema de seguridad sea un factor demasiado importante para el funcionamiento, así que implementar AES en estos sistemas es una de las mejores opciones a pesar de que existen varios algoritmos de encriptación como 3DES,RSA; AES se usa para encriptar la información confidencial de los estados unidos, como se mencionó anteriormente, la información de los usuarios esta en múltiples dispositivos no se puede fallar en ninguna parte en cuestión de seguridad [3].

4. La seguridad de IoT con AES

En la actualidad el avance de la IoT es mayor y su tendencia es a crecer cada vez más, en los avances tecnológicos se pueden observar dispositivos más pequeños que se usan para ayudar en las tareas básicas o más complejas diarias, en donde el usuario final solo ve la información que se comparte entre dispositivos, mas no ve el tratamiento de la información para su buen funcionamiento en este ambiente IoT, sin embargo, es más importante tenerlo en cuenta ya que la información se está usando en diversos

ISSN 1794-211X • e-ISSN 2322-939X • Vol 19, N° 1 (enero-junio 2022). pp. 51-55. Universidad Distrital Francisco José de Caldas-Facultad Tecnológica.

dispositivos, transportándose de un lado a otro por medio de una red lo que hace que esta información se vuelva aún más vulnerable de lo que es, no obstante con la creación de nuevos dispositivos sean pequeños o grandes se implementa el uso del algoritmo AES, este algoritmo de encriptación es uno de los más seguros en la actualidad, por lo tanto, es una buena elección incorporar este algoritmo en cada dispositivo creado, sin importar lo pequeño que sea siempre y cuando maneje información, almacene, capture o la envié, en este caso la información estaría encriptada [4].

Aunque realizar este proceso de encriptación llegue a sobre cargar un poco más los microprocesadores, es importante la seguridad al momento de tratar la información, se debe tener en cuenta que en estos sistemas lo más posible es que se mueva una amplia cantidad de información por consiguiente es necesario la implementación de seguridad, cabe mencionar que además del algoritmo AES se debe proporcionar seguridad a la infraestructura de la red, pero estos puntos se pueden tomar como externos y no de los dispositivos en lo cual se está haciendo énfasis [5].

5. Avances AES en IoT

Los avances que se han generado hablando del algoritmo de encriptación AES son importantes y muy significativos, aunque tal vez este avance no va a la par de los nuevos dispositivos de IoT, se ha estudiado cómo cambiar la estructura de las operaciones algebraicas que utiliza el algoritmo para mejorar la seguridad de este, aunque no se conozcan ataques efectivos, entre más este expuesto el algoritmo puede ser vulnerable por otros medios, por lo tanto hay que mejorar la seguridad del mismo.

El procesamiento de este algoritmo es un tema importante, Inicialmente fue implementado para procesadores grandes de mayor capacidad ocasionando que los microprocesadores que se implementan en IoT sufran un poco, pero no quiere decir que no se puede aplicar en dichos procesadores, con el tiempo se ha trabajado en la forma en que se hacen los procesos, distribuyendo los bloques para ser más óptimos y de esta manera no generen una sobrecarga en el procesador debido a las múltiples tareas que deben realizar [6].

El tener que realizar muchos procesos conlleva un alto consumo de energía, si se habla de un ambiente IoT son muchos los dispositivos que van a estar presentes, si sumamos todo el consumo de energía que realiza cada dispositivo, a futuro se va a generar un alto a nivel de energía, así que se han realizado modificaciones en las cajas Sbox que maneja el algoritmo AES, con el fin de proporcionar un manejo eficiente a los ciclos que necesita el algoritmo para el proceso de encriptar y desencriptar de modo que no genere mucho costo de

ISSN 1794-211X • e-ISSN 2322-939X • Vol 19, N° 1 (enero-junio 2022). pp. 51-55. Universidad Distrital Francisco José de Caldas-Facultad Tecnológica.

procesamiento repercutiendo en un consumo de energía menor.

Un avance de AES en IoT es el manejo de las SBox para manipular las expresiones algebraicas y por lo tanto distribuir los ciclos de una forma óptima, como se han hecho en estudios anteriores, pero en casos separados, incorporar estos cambios en microprocesadores más dedicados implementando este algoritmo, y así mejorar temas de seguridad, consumo de energía y procesamiento.

6. Conclusiones

Es importante el avance de la seguridad en el algoritmo AES dada su implementación en numerosos dispositivos expuestos en una red en donde se transporta excesiva información, aunque el algoritmo no ha presentado ataques exitosos, es de notar que, así como avanzan estos nuevos temas también avanzan las formas de vulnerar estos sistemas.

AES es un algoritmo que brinda seguridad a cualquier sistema en el cual se pueda utilizar procesadores que puedan realizar sus procedimientos en él, a pesar de que puede ser un poco costoso este proceso, muchos microprocesadores pueden implementar AES en su sistema.

Referencias

[1] G. Shan, "Lossless Data Compression for Communication Systems Based on Optical Frequency Discriminator, " *IEEE Access*, vol. 7, pp. 19324-19331, 2019.

[2] Z. Jiang, C. Jin & Z. Wang, "Multiple Impossible Differentials Attack on AES-192, " *IEEE Access*, Vol. 7, pp. 138011-138017, 2019.

[3] K. Bai & C. Wu, "An AES-like cipher and its white-box implementation, " *The Computer Journal*, Vol. 59, no. 7, pp. 1054-1065, 2016.

[4] Y. Sovyn, V. Khoma, & M. Podpora, " Comparison of three CPU-core families for IoT applications in terms of security and performance of AES-GCM, " *IEEE Internet of Things Journal*, vol. 7, no. 1, pp. 339-348, 2019.

[5] S. D. Putra, A. S. Ahmad, S. Sutikno, Y. Kurniawan & A. D. Sumari, "Revealing AES encryption device key on 328P microcontrollers with differential power análisis, " *International Journal of Electrical and Computer Engineering*, vol. 8, no. 6, pp. 5144-5152, 2018.

[6] L. Ramírez y R. Molina, "Prototipo de un Sistema de Comunicación TCP/IP para la detección de fallas en un controlador de tráfico vehicular, " Tesis Ingeniería Electrónica, Universidad Cooperativa de Colombia, 2008.

ISSN 1794-211X • e-ISSN 2322-939X • Vol 19, N° 1 (enero-junio 2022). pp. 51-55. Universidad Distrital Francisco José de Caldas-Facultad Tecnológica.