UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS

Revista Vínculos

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

Revista VÍNCULOS
Ciencia, Tecnología y Sociedad: Un Enlace hacia el Futuro

A+T Actualidad Tecnológica

Aplicaciones actuales de los algoritmos de cifrado Blowfish - Twofish para la protección de los sistemas IoT y computación en la nube

Implementation Current applications of Blowfish – Twofish encryption algorithms for the protection of IoT systems and Cloud Computing

Erika Fernanda Franco Sastre [1], Wilson David Garzón Duque [2], Diana Edelmira Osorio Quiroga [3], Brayan Felipe Fonseca Rocha [4]

Para citar este artículo: E. F. Franco Sastre, W. D. Garzón Duque, D. E. Osorio Quiroga, B. F.Fonseca Rocha, "Aplicaciones actuales de los algoritmos de cifrado Blowfish - Twofish para la protección de los sistemas IoT y computación en la nube", Revista Vínculos, vol 19, no. 1, p-p 56-65, 2022. https://doi.org/10.14483/2322939X.17671

Recibido: 19-12-2021 / Aprobado: 10-03-2022

Resumen: En el presente artículo se da a conocer los conceptos fundamentales de los algoritmos de cifrado (Twofish y Blowfish) y su importancia en el manejo de la privacidad de la información, así como también las técnicas de seguridad que se han implementado por medio de estos algoritmos en el campo de la computación en la nube e Internet de las cosas (IoT).

Palabras clave: Twofish. Blowfish, Internet de las cosas (IoT), Computación en la nube, Seguridad, Cifrado.

Abstract: This paper aims to introduce the fundamental concepts of encryption algorithms (Twofish and Blowfish) and their importance in information privacy management as well as the security techniques that have been implemented by

1 Tecnóloga en Sistematización de Datos, Universidad Distrital Francisco José de Caldas. Correo Electrónico: effrancos@correo.udistrital.edu.co.

2 Tecnólogo en Sistematización de Datos, Universidad Distrital Francisco José de Caldas. Correo Electrónico: wdgarzond@correo.udistrital.edu.co.

3 Tecnóloga en Sistematización de Datos, Universidad Distrital Francisco José de Caldas. Correo Electrónico: deosorioq@correo.udistrital.edu.co

4 Tecnólogo en Sistematización de Datos, Universidad Distrital Francisco José de Caldas. Correo Electrónico: bffonsecar@correo.udistrital.edu.co

means of these algorithms in the field of cloud computing and Internet of Things (IoT).

Keywords: Twofish. Blowfish, Internet of Things (IOT), Cloud Computing, Security, Encryption.

1. Introducción

En la última década ha habido un aumento significativo en el uso de dispositivos y servicios que se conectan o utilizan en internet, lo que ha generado un crecimiento en el número de equipos utilizados por persona. Se calcula que actualmente hay más de 50 mil millones de artículos asociados con el Internet; si tenemos en cuenta la existencia de 6.6 elementos en Internet para cada ser humano [5], el desarrollo que se ha venido dando en el Internet de las cosas (IoT) y la computación en la nube donde cada vez más equipos utilizan una conexión, todo esto genera una circulación de datos mucho más grande y por ende, nuevos desafíos para la protección e integridad de los mismos. Para poder generar esa protección en la información que circula por la red, se han venido desarrollando algoritmos de cifrado en las aplicaciones y en software de los dispositivos que permiten cumplir las características de confidencialidad, integridad y autenticación; dentro de tantos algoritmos utilizados se pueden nombrar a Twofish y Blowfish que son algoritmos de cifrado simétrico y por bloques utilizando una llave compartida en el emisor y receptor.

A continuación, se expondrán conceptos claves de Twofish y Blowfish para entender su funcionamiento, posteriormente se explicará la importancia de estos en la seguridad de los datos de las aplicaciones y dispositivos conectados a internet; luego se analizarán las investigación e implementaciones que se han ido desarrollado en los últimos 10 años de estos dos algoritmos, sus propuestas híbridas con otros algoritmos similares y técnicas de hash para mejorar la seguridad de las aplicaciones de IoT y por último, su implementación en la computación en la nube.

2. Funcionamiento de los algoritmos

Blowfish es un algoritmo de cifrado simétrico, es decir que emplea la misma clave para cifrar y descifrar los mensajes. También es un cifrado de bloques, lo que significa que divide el mensaje en bloques de longitud fija durante el cifrado y el descifrado. La longitud del bloque es de 64 bits y claves de tamaño desde 32 bits a 448 bits [1].

El algoritmo creado en 1993 por Bruce Schneier se desarrolló con el fin de reemplazar el algoritmo DES y a su vez implementar otro estándar de cifrado. A pesar de que han pasado casi 30 años desde el desarrollo del algoritmo Blowfish, se sigue considerando como un algoritmo seguro y difícil de vulnerar, ya que actualmente se desconoce de algún tipo de criptoanálisis

efectivo contra dicho algoritmo. Cabe mencionar que el algoritmo no está patentado, es decir, es de uso libre por tanto se puede acceder, modificar o mejorar su funcionamiento.

Características

- Simple: Blowfish se basa en un diseño simple que es fácil de manipular gracias a que basa sus operaciones en el uso de compuertas lógicas básicas (XOR).
- Rápido: Cifrado Blowfish en microprocesadores de 32 bits.
- Compacto: Blowfish puede ejecutarse en menos de 5 KB de memoria.
- Seguro: Blowfish tiene una longitud de clave variable de hasta un máximo de 448, lo que la hace flexible y segura.

Un cifrado Blowfish consta de lo siguiente:

a) Generación de subclaves: este proceso convierte la clave de hasta 448 bits en subclaves que suman un total de 7168 bits

b) Cifrado de datos: en este proceso se realiza la iteración de una función simple 16 veces. Cada ronda contiene una permutación dependiente de la clave y una sustitución de claves y datos.

c) Cajas S: los datos de 32 bits se subdividen en cuatro palabras de 8 bits y estos se ingresan a los bloques de permutación qi, posteriormente las salidas se unen y se blanquean con las subclaves Si.

d) Función F: dentro del algoritmo se define una función que se presenta después de las operaciones XOR, tomando los valores resultantes y reemplazándolos mediante las cajas de sustitución (caja S ó S-Box). El valor inicial que recibe la función son 32 bits, que después se separa en 4 bloques de 8 bits, en dichos bloques se realizan operaciones lógicas de XOR y sumatorias, además de emplear el concepto de Caja-S.

e) Texto plano: contiene los caracteres originales, los valores que antes de entrar al algoritmo se mantienen tal cual se ingresaron.

f) Texto cifrado: una vez el texto plano pasa por el algoritmo, realiza un número de iteraciones pertinentes dentro de este, para finalmente obtener un texto ilegible muy alejado del resultado original, con el fin de mantener encriptado el mensaje de entrada hasta que llegue a su destino.

2.1. Funcionamiento Twofish

Es un método de criptografía simétrica con cifrado por bloques desarrollado por Counterpane Labs y presentado al concurso del NIST que buscaba un sustituto para DES (el concurso AES). El tamaño de bloque en Twofish es de 128 bits y el tamaño de clave puede llegar hasta 256 bits [6].

Twofish encripta 128 bits de texto plano P, en 128 bits de texto cifrado C, a través de 16 rondas controladas por 40 subclaves de 32 bits. La clave de usuario K es variable y puede ser de 128, 192 o 256 bits [4].

Un cifrador Twofish consta de lo siguiente:

a. Blanqueo: se toma un bloque de texto plano de 128 bits agrupado en 4 palabras de 32 bits cada uno, y se realiza la operación XOR bit a bit con 4 subclaves (de 32 bits cada 57 una) [4].

b. 16 Ronda: la ronda de cifrado Twofish consta de una red Feistel, o función F y unas operaciones adicionales de rotación cíclica de un bit y XOR [4].

c. Redes de Feistel: se trata de un método general para transformar cualquier función F en una permutación. El fundamento de las redes de Feistel se basa en un mapeo, dependiente de la clave, de un string de entrada en otro de salida [7]. Es el bloque más importante del algoritmo, se compone de Rotación cíclica de 8 bits a la izquierda, Función G, Rotación cíclica de 8 bits a la izquierda, Transformada pseudo-Hadamard (PHT) y Suma módulo 232 [4].

d. Función G: se compone de dos partes, primero se realiza una sustitución a los datos a través de Cajas-S y posteriormente se realiza una operación matemática con los datos utilizando una matriz denominada MDS.

e. Transformada pseudo-Hadamard: la transformada pseudo-Hadamard, ó PHT, corresponde a la implementación de las ecuaciones y dos datos de 32 bits cada uno.

$$a' = a + b \bmod 2^{32}$$
$$b' = a + 2b \bmod 2^{32}$$

Twofish usa una PHT de 32 bits para mezclar las salidas de sus 2 funciones paralelas de 32 bits.

3. Importancia en la seguridad de la información

En el uso de aplicaciones web o móviles, la seguridad de la información y cómo esta se transmite a través de redes alámbricas e inalámbricas suelen ser los blancos de ataque de personas externas al mensaje que pretenden robar, desviar o descifrar la información que se está enviando. Se han evidenciado situaciones en las cuales durante la transmisión del mensaje estas personas “inyectan” información que no está contemplada en el mensaje original, cambiando el propósito y orden de envío de la información.

Por estas y otras razones, mantener la seguridad y confidencialidad de la información durante su envío es fundamental dentro distintas aplicaciones tecnológicas; la criptología ofrece distintos algoritmos para

ISSN 1794-211X • e-ISSN 2322-939X • Vol 19, N° 1 (enero-junio 2022). pp. 56-65. Universidad Distrital Francisco José de Caldas-Facultad Tecnológica.

mantener el texto plano seguro hasta su recepción.

El algoritmo Blowfish junto con el Twofish siguen siendo muy utilizados en aplicaciones de seguridad, actualmente son conocidos como algoritmos más fuertes ya que no son susceptibles a ningún ataque razonable, pues los intentos más exitosos de vulnerar dicho algoritmo han requerido ataques exhaustivos.

El gusto de aplicar este algoritmo en diversos esquemas de hardware y software se da a partir de su fácil implementación y la facilidad con la cual se pueden realizar cambios en el algoritmo. Se han propuesto esquemas en hardware en donde a través de la programación de circuitos, se implementa el algoritmo de Blowfish con algunas variaciones dentro de sus sentencias, con el fin de adaptarse y mejorar el proceso de cifrado mientras el dispositivo hace el menor uso posible de recursos. Se han propuesto circuitos y crypto chip con sentencias que gestionan la autenticación y realizan más o menos ciclos del algoritmo Blowfish modificado.

El crecimiento acelerado de redes tecnológicas y productos móviles que requiere de conexión a la nube o que interfieren en el comportamiento de otros dispositivos, es directamente proporcional a la necesidad de mantener un esquema de seguridad fiable. El diseño y mejora de algoritmos de cifrado va a continuar existiendo mientras se sigan desarrollando dispositivos que requieren confiabilidad, escalabilidad, seguridad y fiabilidad dentro de sus sistemas.

4. Aplicaciones actuales

Actualmente, se han venido utilizando algoritmos de cifrado en aplicaciones con gran demanda, como es el Internet de las cosas (IoT), la computación en la nube, aplicaciones de aprendizaje automático, dispositivos móviles, aplicaciones web, entre otras, ya que debido a la cantidad de usuarios conectados a estas herramientas y tecnologías, el tema de seguridad ha tomado mucha más fuerza y relevancia en la privacidad de la información. Sólo es responsable de la distribución de recursos a las aplicaciones de ejecución. La disposición que establezcan los dispositivos es una estructura enchufable para asignar las propiedades del clúster en muchas situaciones. Sea provisional en la situación de uso y condición de usuario, los administradores pueden seleccionar un planificador fijo unidireccional, planificador de capacidad o planificador justo. Actualmente, se hace uso de los tres planificadores con el fin de solventar las soluciones de IoT en varios escenarios tecnológicos dentro de la población.

A continuación, se listan algunas investigaciones y desarrollos en este tipo de temas realizados en los últimos años.

ISSN 1794-211X • e-ISSN 2322-939X • Vol 19, N° 1 (enero-junio 2022). pp. 56-65. Universidad Distrital Francisco José de Caldas-Facultad Tecnológica.

4.1. Seguridad en IoT

Es innegable que el Internet de las Cosas (IoT) ha empezado a afectar muchos aspectos de nuestra vida. En el futuro se espera que esto siga creciendo, pero claro está, su gran auge y potencial avance supone un riesgo mayor en términos de seguridad; cualquier dispositivo que utilice IoT es vulnerable durante todo el proceso de uso; en el proceso de transferencia de datos estos dispositivos pueden sucumbir ante amenazas que van desde problemas de autenticación y acceso, hasta robo de datos e información confidencial. El peligro se presume aún mayor teniendo en cuenta que debido a este gran auge, son muchas las empresas que implementan de forma acelerada IoT descuidando incluso aspectos básicos de seguridad.

Es por esto que, en los últimos años ha crecido la urgencia por implementar algoritmos criptográficos de cifrado simétricos como Twofish y Blowfish en aplicaciones IoT; varias investigaciones se han encargado de realizar estudios de comparación entre distintos algoritmos para determinar cuál podría ser más seguro y eficiente, pero también cuál supone el uso de menos recursos. Manju Suresh y Neema M. de la Adi Shankara Institute Of Engineering & Technology de la India en su investigación advierten que existen riesgos de seguridad en cada una de las tres capas presentes durante el intercambio de información entre dispositivos, proponen el uso del algoritmo Blowfish modificado como mecanismo para mejorar tanto el cifrado como el rendimiento; para verificar esta efectividad comparan este algoritmos con algoritmos tipo RSA, AES y DES; al final demuestran que en efecto el uso del algoritmo Blowfish mejora el tiempo de ejecución, el rendimiento y el uso de memoria [13].

Una investigación un poco más reciente realizada en el Computer Science Department de la Ghana Technology University, también ante la preocupación en términos de seguridad de las aplicaciones IoT, propone el uso del algoritmo TwoFish junto con DHE; a lo largo del estudio se evidencia que el uso único del protocolo DHL resulta insuficiente, puesto que se limita solo al uso de claves dejando de lado el aspecto que tiene que ver con la autenticación, es por eso que se decide incorporar el AES sin dejar de lado DHE, esto quiere decir que se propone un uso conjunto de los dos algoritmos para mejorar aspectos como la validación y verificación aumentando tanto la seguridad como la confidencialidad; es así como el uso de Twofish junto con AES y DHE resulta óptimo para garantizar un intercambio seguro de datos en aplicaciones IoT. Al final de este estudio podemos rescatar la idea de mejorar la seguridad y eficiencia con el uso de algoritmos híbridos [14].

Algunos estudios también han demostrado que el uso de algoritmos híbridos es adecuado para usar en Smartphones; recordemos que hoy por hoy el uso del smartphone se ha vuelto vital en el desarrollo

ISSN 1794-211X • e-ISSN 2322-939X • Vol 19, N° 1 (enero-junio 2022). pp. 56-65. Universidad Distrital Francisco José de Caldas-Facultad Tecnológica.

del IoT y, por lo tanto, debe pensarse en buscar mecanismos de seguridad que sean eficientes y que al mismo tiempo tengan en cuenta limitaciones de los dispositivos, ya que no es lo mismo la capacidad de una Tablet, un smartphone o la capacidad de grandes computadoras. Es así como un estudio publicado en 2016 por el Department of Computer Engineering del Sankalchand Patel College of Engineering en la India resalta el uso de un enfoque híbrido, en este caso el uso del algoritmo Blowfish y ECC para la seguridad de smartphones, demostrando así que este tipo de enfoque supone el uso de pocos recursos en dispositivos pequeños y mejora la eficiencia [15].

Otra de las investigaciones realizadas recientemente por el Department of Information Technology de la Altinbas University vuelve de nuevo al uso del algoritmo Blowfish como un algoritmo ligero y sobre todo estable que mejora la seguridad, el rendimiento y la confidencialidad del IoT [5].

Con todo lo anterior es válido señalar que aún no hay un consenso sobre qué algoritmo es más recomendado, pero lo que sí es cierto es que Blowfish y Twofish van a la cabeza. Por otro lado, también es importante recalcar el hecho de que el uso de alguno de estos dos algoritmos junto con otros de tipo asimétrico (algoritmos híbridos) constituye un uso aún en investigación, pero que promete por el momento, ser la clave para lograr tanto sistemas y aplicaciones seguras, como económicas (en términos de energía), con mejor rendimiento, más rápidas y, otro aspecto que es muy importante, una buena compatibilidad entre dispositivos.

4.2 Seguridad computación en la nube

Con el auge que han tenido hoy en día los servicios de la nube, se ha vuelto indispensable la seguridad y privacidad de los datos que se almacenan en estas plataformas, es por eso que se han venido desarrollando proyectos e investigaciones referente al tema de cifrado de datos con los algoritmos de Twofish y Blowfish; algunos de esos proyectos se han enfocado en la combinación de algoritmos, como es el caso de una investigación hecha en el School of Computer Science and Engineering de Singapur; en este estudio se prueba que la combinación de los algoritmos DES y Blowfish permiten un alto nivel de seguridad y resistencia frente a diversos ataques de criptografía, también se concluye que Blowfish puede llegar a ser más rápido que DES [8].

Otro proyecto importante es uno realizado por el Department of Computer Science and Engineering en G. Pulla Reddy Engineering College (Autonomous): Kurnool, AP, India, aquí se expone un algoritmo de cifrado basado en Blowfish y gestión de llaves en la seguridad de la nube, el artículo aborda algunas problemáticas que se presentan actualmente en la nube y cómo, a partir de la implementación del algoritmo de Blowfish con Byzantine fault tolerance algorithm (BFT)

ISSN 1794-211X • e-ISSN 2322-939X • Vol 19, N° 1 (enero-junio 2022). pp. 56-65. Universidad Distrital Francisco José de Caldas-Facultad Tecnológica.

en procesos de encriptación y desencriptación, puede ayudar a mitigar algunas de las vulnerabilidades presentes en la nube en software como servicio (SaaS) [9].

Otro proyecto interesante, pero más enfocado a la seguridad en la nube con relación a la analítica de datos, (un servicio que también ofrece la computación en nube), es la implementación de un laboratorio para brindar seguridad de datos con análisis predictivo a través del algoritmo de Twofish; en este se describe la elaboración de un software que será usado por los laboratorios para almacenar información de los pacientes en una base de datos MySql en la nube; desarrollado en PHP y con algoritmos de Java su uso permite que se almacenen informes de los pacientes por bloques mediante encriptación y recuperación de los mismos mediante cifrado. Esto permite proteger la integridad de los datos de los pacientes y además mejora el rendimiento y costo de almacenamiento en la nube [10].

Otro proyecto enfocado en la seguridad en la nube fue desarrollado en la India por el "Department of Computer Science and Engineering, SNS College of Engineering, Coimbatore, Tamilnadu", el interés principal parte del problema sobre cómo garantizar la seguridad de los datos en la nube en términos de compatibilidad, integridad, confidencialidad y privacidad. Los autores en este sentido identifican fallas de este tipo de algunas aplicaciones en la nube y con sistemas de seguridad que, debido al aumento de almacenamiento en la nube, son cada vez más susceptibles a ser vulnerados o pirateados, por lo anterior, proponen un tipo de cifrado simétrico (Blowfish) para el almacenamiento seguro de los datos y al mismo tiempo para la reducción del tiempo de procesamiento y entrega junto con la precisión.[11].

Con relación a la seguridad de datos médicos, al igual que uno de los proyectos mencionados anteriormente, se realizó una investigación en "Department of Computer and Information Science Annamalai University" en Indonesia donde se implementó un algoritmo de cifrado de datos híbrido para una transmisión segura de datos médicos en un entorno de la nube. El modelo propuesto en este artículo se basa en la integración de la Transformada Discreta Wavelet de dos niveles (DWT 2D) con un esquema híbrido de encriptación, este esquema integra el algoritmo Blowfish y el Twofish [12].

5. Conclusiones

La implementación de sistemas de cifrado con algoritmos como Twofish y Blowfish en aplicaciones IoT y computación en la nube permiten generar una mayor seguridad y fiabilidad en el envío de la información que se generan en estas.

Se dieron a conocer las soluciones de seguridad a los problemas existentes en la

ISSN 1794-211X • e-ISSN 2322-939X • Vol 19, N° 1 (enero-junio 2022). pp. 56-65. Universidad Distrital Francisco José de Caldas-Facultad Tecnológica.

actualidad de carácter generalizado, pero con un enfoque detallado para los dispositivos IoT, estableciendo una directa relación entre los algoritmos de cifrado tales como Blowfish y Twofish y las tecnologías de IoT y computación en la nube.

Actualmente se ha venido desarrollando políticas de seguridad para los sistemas IoT y computación en la nube y es innegable que seguirán saliendo más en el futuro para mejorar la privacidad de la información teniendo en cuenta que es un aspecto muy sensible y de mucha preocupación en este tipo de sistemas que cada día se ve en aumento.

Referencias

[1] B. Gatliff, "Encrypting data with the Blowfish algorithm - Embedded.com," *Embedded.com*, 2021. [Online]. Available: https://www.embedded.com/encrypting-data-with-the-blowfish-algorithm.

[2] "Blowfish Algorithm with Examples - GeeksforGeeks," *GeeksforGeeks*, 2021. [Online]. Available: https://www.geeksforgeeks.org/blowfish-algorithm-with-examples/

[3] R. Mishra and R. Mishra, "Blowfish Encryption Algorithm - Everything You Need To Know - Tech4EN," *Tech4EN, 2021*. [Online]. Available: https://tech4en.org/blowfish-encryption-algorithm/

[4] O. Casas, Implementación de los cifradores de bloque Rijndael, Serpent, Mars, Twofish y RC6 para su uso en sistemas embebidos, 1st ed. Cali, Colombia: La Umbría, carretera a Pance, 2010, pp. 55-64.

[5] M. J. Saddam, A. A. Ibrahim and A. H. Mohammed, "A Lightweight Image Encryption And Blowfish Decryption For The Secure Internet Of Things," 2020 4th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT), Istanbul, Turkey, 2020, pp. 1-5.

[6] "Glosario", Ccn-cert.cni.es, 2021. [Online]. Available: https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/400-Guias_Generales/401-glosario_abreviaturas/index.html?n=936.html

[7] L. Sanjuan, "Criptografía I," 2012. [Online]. Available: http://materias.fi.uba.ar/6669/alumnos/1999/aes.pdf

[8] K. Santoso, M. Muin and M. Mahmudi, "Implementation of AES cryptography and twofish hybrid algorithms for cloud," *Journal of the Gujarat Research Society*, 2020.

[9] B. T. Reddy, K. B. Chowdappa, & S. R. Reddy, "Cloud Security using Blowfish and Key Management Encryption Algorithm," *International Journal of Engineering and Applied Sciences*, vol. 2, no. 6, Junio de 2015.

[10] A. Devi, B. S. Ramya, "Two fish Algorithm Implementation for lab to provide data security with predictive analysis, " *International Research Journal of Engineering and Technology*, vol. 4, no. 5, pp. 3033-3036, 2017

[11] V. K. R. Gangireddy, S. Kannan, K. Subburathinam, "Implementation of enhanced blowfish algorithm in cloud environment," *Journal of Ambient Intelligence and Humanized Computing*, pp. 1-7, 2020.

[12] B. Pushpa, "Hybrid Data Encryption Algorithm for Secure Medical Data Transmission in Cloud Environment," 2020 Fourth International Conference on Computing Methodologies and Communication (ICCMC), Erode, India, pp. 329-334, 2020.

[13] M. Suresh, M. Neema, "Hardware implementation of blowfish algorithm for the secure data transmission in Internet of Things, " *Procedia technology*, vol. 25, pp. 248-255, 2016.

[14] B. T. Asare, K. Quist-Aphetsi & L. Nana, "Secure Data Exchange Between Nodes in IoT Using TwoFish and DHE," 2019 International Conference on Cyber Security and Internet of Things (ICSIoT), Accra, Ghana, pp. 101-104, 2019.

[15] P. Patel, R. Patel, & N. Patel, "Integrated ECC and Blowfish for smartphone security," *Procedia Computer Science*, vol. 78, pp. 210-216, 2016.