Artículos

Principales técnicas criptográficas aplicadas a la seguridad de la información en IoT: una revisión sistemática

Olivarez Geronimo Dionicio, Percy; Lezcano Gil, Alfredo José; Mendoza De Los Santos, Alberto Carlos

Percy Olivarez Geronimo Dionicio
t1063300120@unitru.edu.pe
Universidad Nacional de Trujillo, Perú
Alfredo José Lezcano Gil
Universidad Nacional de Trujillo, Perú
Alberto Carlos Mendoza De Los Santos
Universidad Nacional de Trujillo, Perú

Ingenio Tecnológico
Universidad Tecnológica Nacional, Argentina
ISSN-e: 2618-4931
Periodicidad: Frecuencia continua
vol. 5, e041, 2023
ingenio@frlp.utn.edu.ar

Recepción: 03 Octubre 2023
Aprobación: 30 Noviembre 2023
Publicación: 30 Noviembre 2023

URL: http://portal.amelica.org/ameli/journal/266/2663842005/

Resumen: Este artículo de revisión proporciona una visión exhaustiva de las principales técnicas criptográficas aplicadas a la seguridad de la información en el Internet de las Cosas (IoT) analizando diferentes artículos de investigación recopilados de diversas bases de datos académicas, incluyendo MDPI, Scopus Y ScienceDirect.
El cifrado de curva elíptica se encontró como una opción para entornos donde se tienen pocos recursos y se quiere se lo más eficiente posible, mientras que el uso de AES es fundamental para priorizar la seguridad ya que esta técnica de cifrado brinda confiabilidad al ser un estándar con muchas investigaciones que avalan su efectividad en la seguridad de datos en IoT. Por último se muestra al cifrado hash que permite tener datos más integrados y totalmente auténticos dentro de los entornos IoT, acoplándose a otras técnicas de cifrado como ECC, AES, RSA, etc.
Los resultados obtenidos también revelan la necesidad de avanzar en la exploración de enfoques de cifrado cuántico y técnicas de aprendizaje automático para lograr una detección y prevención efectiva de amenazas en tiempo real en entornos IoT, así como también es crucial evaluar la eficacia de estas técnicas en escenarios IoT más diversos y heterogéneos.

Palabras clave: Criptografía, Seguridad de la información, Internet de las Cosas, Aplicaciones.

Abstract: This review article provides a comprehensive overview of the main cryptographic techniques applied to information security in the Internet of Things (IoT), analyzing various research articles gathered from diverse academic databases, including MDPI, Scopus, and ScienceDirect.
Elliptic curve encryption was identified as an option for environments with limited resources, aiming to be as efficient as possible. Meanwhile, the use of AES is crucial to prioritize security, as this encryption technique provides reliability by being a standard with numerous studies supporting its effectiveness in securing data in IoT. Finally, hash encryption is highlighted for enabling more integrated and completely authentic data within IoT environments, complementing other encryption techniques such as ECC, AES, RSA, etc.
The results obtained also reveal the need to advance exploration into quantum encryption approaches and machine learning techniques to achieve effective real-time detection and prevention of threats in IoT environments. It is crucial to evaluate the effectiveness of these techniques in more diverse and heterogeneous IoT scenarios.

Keywords: Cryptography, Security of the information, Internet of Things, Application.

Introducción

La seguridad de la información en el Internet de las cosas (IoT) es un tema crítico, debido a una rápida expansión del Internet de las Cosas que ha generado un entorno digital interconectado, donde dispositivos inteligentes recopilan, transmiten y utilizan datos de manera continua, impulsando la eficiencia y la comodidad para los usuarios, pero simultáneamente ha aumentado los riesgos de seguridad en la manipulación y transmisión de información sensible ya que los dispositivos conectados pueden presentar vulnerabilidades ante ataques cibernéticos. Según un estudio de IBM (2023), el número de ataques dirigidos a dispositivos IoT se incrementó en un 400% entre 2018 y 2020, y esta tendencia continúa en los años siguientes. Esto demuestra que la revolución del Internet de las Cosas (IoT) ha permeado nuestra vida cotidiana, integrando una multitud de dispositivos, desde termostatos hasta vehículos en la red global. No obstante, la proliferación de estos dispositivos interconectados ha suscitado preocupaciones significativas entorno a la seguridad.

Los dispositivos IoT pueden ser susceptibles a una variedad de ataques, incluyendo el robo de credenciales, la explotación de vulnerabilidades del firmware, y los ataques de denegación de servicio distribuido (DDoS), entre otros. Estos ataques pueden comprometer la confidencialidad, integridad y disponibilidad de la información, así como la privacidad y seguridad de los usuarios y organizaciones. Para contrarrestar estos riesgos, se requieren técnicas criptográficas robustas que aseguren la autenticación, autorización, encriptación y cifrado de los datos intercambiados entre los dispositivos IoT y las redes a las que están conectados.

En este contexto, este artículo se centra en la siguiente pregunta de investigación ¿Cuáles son las técnicas criptográficas más efectivas y relevantes para garantizar la seguridad de la información en entornos del Internet de las Cosas (IoT)? A pesar de la abundancia de investigaciones centradas en diversas técnicas criptográficas destinadas a mejorar la seguridad de la información en el contexto IoT, la selección de una técnica criptográfica específica para su aplicación en un contexto real puede resultar desafiante. Por lo tanto, este artículo se enfoca en el análisis de técnicas criptográficas en el contexto del IoT con el objetivo principal de proporcionar una visión integral y simplificada de las técnicas empleadas en situaciones reales de diversos campos de aplicación en entornos de IoT, evaluando su eficacia y aplicabilidad en la mejora de la seguridad de la información.

1. Aplicaciones de IOT

Según Abdur et al. (2017), las principales aplicaciones del Internet de las Cosas (IoT) buscan configurar un entorno inteligente y dispositivos autónomos para áreas como la vida, objetos, salud y ciudades inteligentes. El IOT tiene principalmente aplicaciones en los siguientes campos:

1.1. IOT en las industrias

El IoT ha permitido la creación de sistemas y aplicaciones significativas. Por ejemplo, en un sistema de transporte inteligente IoT, una persona autorizada puede monitorear la ubicación y el movimiento de un vehículo, así como predecir su ubicación futura y el tráfico vial. Inicialmente, el término IoT se usaba para identificar objetos únicos con RFID, luego los investigadores han relacionado el término IoT con sensores, dispositivos del Sistema de Posicionamiento Global (GPS), dispositivos móviles y actuadores.

1.2. IOT en los Dispositivos médicos

Los sistemas de salud utilizan ampliamente dispositivos del Internet de las Cosas (IoT) para supervisar y evaluar a los pacientes. Los Dispositivos Médicos Personales (PMDs) son dispositivos electrónicos pequeños que se implantan en el cuerpo del paciente o se adhieren a él. Estos dispositivos, que se estimó que tendrían un valor de mercado de alrededor de 17 mil millones de dólares en 2019, se comunican con una estación base a través de una interfaz inalámbrica. Esta estación base se utiliza para leer el estado del dispositivo, informes médicos, modificar parámetros del dispositivo o actualizar su estado.

1.3. IOT en los servicios de hogares

Los servicios de hogares inteligentes están en constante crecimiento ya que los dispositivos digitales pueden comunicarse eficazmente entre sí utilizando direcciones del Protocolo de Internet (IP). Todos los dispositivos de un hogar inteligente están conectados a internet, a medida que aumenta el número de dispositivos en el entorno del hogar inteligente, también aumentan las posibilidades de ataques maliciosos, sin embargo, si los dispositivos del hogar inteligente operan de manera independiente, las posibilidades de ataques maliciosos disminuyen.

Actualmente, los dispositivos del hogar inteligente pueden ser accedidos a través de internet en cualquier lugar y en cualquier momento, lo que aumenta las posibilidades de ataques maliciosos en estos dispositivos.

2. Capas de sistemas IOT

Según Caraveo M. et al. (2023), existen 4 capas principales en todo sistema de internet de las cosas (IoT), estas capas son:

2.1. Capa de Percepción

Esta capa desempeña un papel fundamental al permitir la identificación de elementos que pueden conectarse a un sistema IoT y que involucran la utilización de sensores y actuadores. Su principal tarea radica en recolectar datos relevantes provenientes de objetos o dispositivos IoT para posteriormente convertirlos en un formato digital adecuado.

2.2. Capa de Conectividad

En esta etapa, se establece la comunicación a través de protocolos como TCP o mediante una puerta de enlace que actúa como un enlace entre redes LAN y WAN. Esta capa opera en conjunto con la capa de procesamiento y se asemeja a la capa de red en un modelo de tres capas de IoT. Su objetivo principal es facilitar la interconexión de dispositivos y posibilitar avances tecnológicos, como el uso de servicios en la nube o la computación en el borde, con el propósito de mejorar el rendimiento del sistema.

2.3. Capa de Procesamiento

Esta capa representa el núcleo del IoT, donde los datos obtenidos de los sensores son sometidos a análisis, procesamiento y posterior almacenamiento. Aquí se encuentran la unidad de procesamiento y el sistema

de almacenamiento. En esta fase se llevan a cabo dos acciones cruciales: la acumulación de datos (mediante almacenamiento en la nube para grandes volúmenes de información) y la abstracción de datos (adecuación para su presentación a usuarios finales). La computación en la nube y la informática en el borde desempeñan un papel esencial en esta capa. La placa de desarrollo tiene la capacidad de procesar datos en tiempo real en el lugar donde se recolectan los datos de los sensores, transmitiendo solamente la información relevante al servidor.

2.4. Capa de Aplicación

En esta fase, se ofrecen servicios de usuario dirigidos a aplicaciones de IoT, como hogares inteligentes y salud conectada. Los datos que fueron procesados en la capa anterior se presentan al usuario mediante plataformas de software o aplicaciones móviles diseñadas específicamente para sistemas IoT, en el formato requerido, que puede incluir elementos visuales como gráficos y otros recursos, tal como se muestra en la figura 1.

3. Algoritmos de criptografía

Los algoritmos de cifrado se pueden clasificar en 3 grandes grupos, las cuales son:

3.1. Algoritmos de cifrado pública (Asimétrica)

Algoritmo Rivest Shamir Adleman (RSA): El algoritmo RSA, desarrollado por Rivest, Shamir y Adleman, es un destacado sistema criptográfico de clave asimétrica que aborda el desafío de seguridad de factorizar números grandes en factores primos para obtener una clave secreta. Su ventaja está en el nivel de dificultad para factorizar números no primos en factores primos, el algoritmo sugiere el uso de valores a y b con más de 100 dígitos, lo que resulta en un producto ($n = a \times b$) que supera los 200 dígitos la cual lo hace muy compleja que personas no autorizadas calculen la clave de descifrado. (Liestyowati Dwi, 2020).

Algoritmo de curva elíptica (ECC): La criptografía de curva elíptica (ECC) representa la técnica más avanzada y reciente en el campo de la criptografía, el cual su aplicación, especialmente a través del algoritmo de firma digital de curva elíptica (ECDSA), se destaca en la mejora de la seguridad en redes de comunicación abiertas y en la autenticación de usuarios en la Era Digital Moderna (EDM). Los usuarios de EDM, que participan en diversas tecnologías como redes sociales, almacenamiento en la nube y la industria del Internet de las cosas (IoT), demandan un entorno seguro que preserve su privacidad. La criptografía es esencial para proteger la transmisión de datos y la transferencia de información contra robos y ataques en canales abiertos (Ullah et al., 2023)

3.2. Algoritmos de cifrado privado (Simétrica)

Algoritmo Estándar de cifrado Avanzado (AES)

Este algoritmo se emplea como tecnología esencial para salvaguardar información confidencial en diversas aplicaciones. Su implementación principal se realiza en software, cifrando datos sensibles para sistemas específicos. En el ámbito de la fabricación inteligente y sistemas caóticos, se recurre a una variante basada en el estándar ligero de cifrado avanzado (LAES) para gestionar la seguridad. Este método analiza el contenido del texto protegido, empleando un algoritmo híbrido basado en AES para reforzar la seguridad en entornos caóticos (Huo et al., 2023).

Algoritmo Triple DES (3DES)

En un estudio reciente, se destacó la vulnerabilidad del algoritmo de cifrado Triple DES (3DES) mediante ataques de búsqueda exhaustiva utilizando el estudio GPU RTX 3070, se logró realizar 94.4 millones de búsquedas de claves por segundo para 3DES, lo que sugiere una posible vulnerabilidad del cifrado con claves de 112 bits. Este resultado plantea la posibilidad de romper la seguridad de 112 bits de 3DES en aproximadamente 8 años con una GPU RTX 3070, por lo tanto, se destaca la vulnerabilidad de algoritmos criptográficos ligeros, como 3DES, que emplean claves cortas y son susceptibles a ataques de fuerza bruta (Tezcan, 2022).

3.3. Funciones HASH

Las funciones hash son de vital importancia para asegurar la integridad y seguridad de mensajes de longitud variable en sistemas de comunicación, debido a que los enfoques tradicionales de criptografía simétrica y asimétrica tienen limitaciones en este aspecto, lo que ha llevado a la necesidad que las funciones hash emergen como elementos cruciales para mejorar la seguridad en aplicaciones y protocolos criptográficos. Estas funciones no solo aceptan mensajes de longitud variable, sino que también generan valores hash de longitud fija, proporcionando así una capa adicional de integridad y autenticación. La necesidad de estas funciones se fundamenta en requisitos esenciales como la resistencia a colisiones, resistencia previa a la imagen y segunda resistencia de la preimagen, que son fundamentales para garantizar la robustez de la seguridad criptográfica (Ullah et al. ,2023)

4. Desafíos en los sistemas de IoT:

Según Bhatt & Sharma (2019) y Martínez & Cruz (2018), los desafíos que tiene los sistemas de internet de las cosas (IOT) son los siguientes:

Actualizaciones de Seguridad: Mantener dispositivos IoT actualizados con los últimos parches de seguridad y algoritmos criptográficos es un desafío, ya que muchos de ellos no son fácilmente accesibles o actualizables una vez que están desplegados.
Responsabilidad Legal: No existe una ley o normativa que controle y respalde la seguridad de los datos utilizados en los entornos IoT de las empresas, como tampoco existen estándares para la implementación, desarrollo y uso de los mismos.
Privacidad del Usuario: La criptografía desempeña un papel importante en la protección de la privacidad del usuario en el IoT. Garantizar que los datos personales se protejan de manera efectiva y se compartan solo cuando sea necesario es un desafío constante.
Escalabilidad: A medida que el número de dispositivos IoT aumenta, la gestión de la seguridad como también la criptografía a gran escala se vuelve cada vez más compleja y desafiante.
Altos costos en IoT: Debido a que los dispositivos IoT son aún novedosos, existe un alto consumo de recursos propios para mantenerse en ejecución, como el alto consumo de energía, esto con el tiempo debería mejorarse sin embargo sigue siendo un desafío para las empresas en la actualidad.

Metodología

1. Fundamentos de la metodología

Este estudio llevará a cabo una revisión sistemática siguiendo la metodología PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) como marco de referencia. Según Page et al. (2021), esta metodología proporciona un marco que simplifica la ejecución de un estudio sistemático fundamentado en investigaciones académicas anteriores.

Su enfoque estructurado mejora la calidad y la transparencia de la investigación al proporcionar pautas claras para la planificación, ejecución y presentación de la revisión. Adoptamos PRISMA en nuestro estudio para garantizar una investigación rigurosa y objetiva, minimizando el sesgo de selección y mejorando la calidad de nuestro informe.

2. Criterios de Inclusión y exclusión

Para asegurar la selección de los artículos más pertinentes y adecuados para nuestra revisión, establecemos los siguientes criterios de inclusión y exclusión tal como se muestra en la tabla 1 y tabla 2 respectivamente.

TABLA 1
Criterios de inclusión

N°	Criterio de Inclusión
CI1	Incluir solamente artículos de investigación y de revisión
CI2	Incluir artículos que hayan sido publicadas en el periodo (2019 -2023)
CI3	Incluir los artículos de idioma inglés o español

TABLA 2
Criterios de exclusión

N°	Criterio de exclusión
CE1	Excluir los artículos que no tienen "acceso libre"
CE2	Excluir artículos que no contengan las palabras claves "Técnicas criptográficas" y "Internet de las cosas (IOT)".
CE3	Excluir aquellos artículos que no se centren en un ámbito tecnológico y que no traten específicamente sobre la seguridad de la información.

3. Proceso de recolección de información

La búsqueda de información se llevó a cabo en bases de datos académicas ampliamente reconocidas como Scopus, ScienceDirect y MDPI, las cuales albergan una vasta colección de artículos académicos. Posteriormente, se implementaron los criterios de exclusión, lo que nos permitió identificar y filtrar los artículos pertinentes a nuestro tema de investigación, tal como se muestra en la figura 2.

Finalmente, seleccionamos los artículos que serán objeto de un análisis exhaustivo. Estos fueron elegidos debido a su alta relevancia y su significativa aportación a nuestro campo de investigación, por lo que serán sometidos a un análisis detenido y riguroso.

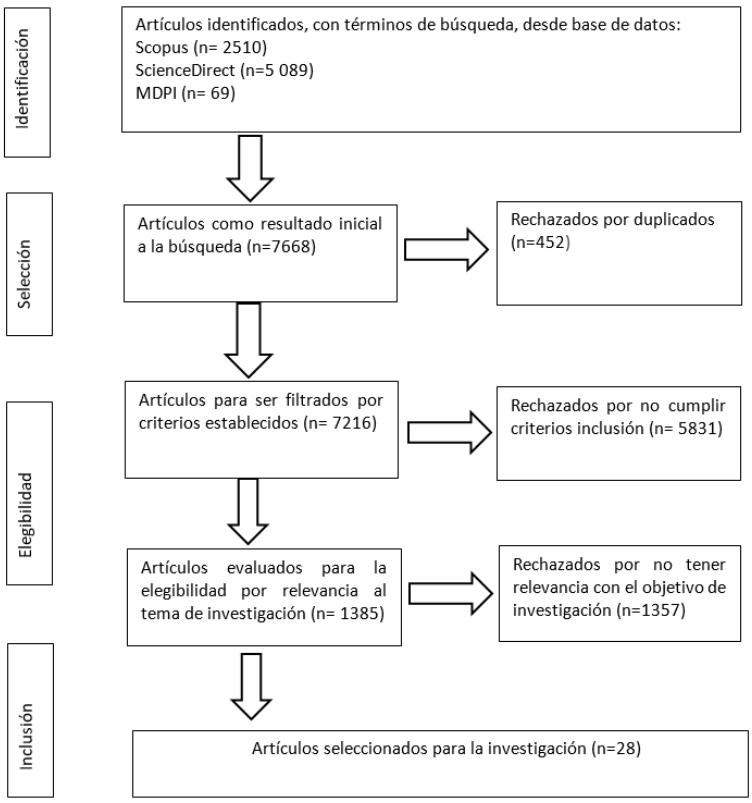

FIGURA 2
Esquema del proceso de recopilación de datos

TABLA 3
Resumen de Búsqueda en bases de datos

Base de datos	Término de búsqueda	Resultados	Seleccionados
SCOPUS	cryptography AND security AND information AND "internet of things"	2, 510	9
ScienceDirect	"Cryptography" and ("Internet of Things" or "IoT") and "security"	5, 089	15
MDPI	Cryptography AND Internet of Things AND security AND data	69	4

Además, es importante destacar que la mayoría de las investigaciones sobre este tema provienen de autores residentes del país de la India. En nuestro estudio, casi el 50% de los autores pertenecen a este país, tal como se muestra en la figura 3.

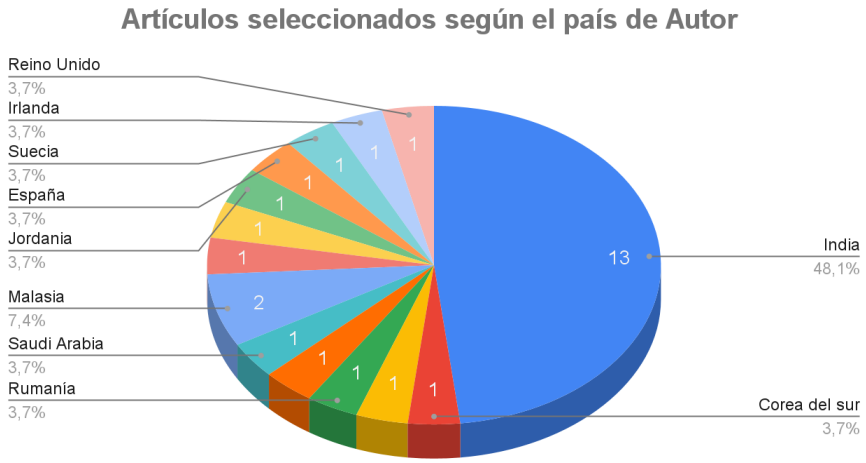

FIGURA 3
Artículos publicados según el país de autor
Elaboración propia

Resultados

TABLA 4
Soluciones criptográficas en Seguridad de IoT

ID	Autores y Fecha	Soluciones criptográficas	Conclusión
A1	**Hussain, S., & Mohideen S, P. (2023).**	sistema de Detección de Mensajes Criptográficos Sospechosos (SCMD)	Este marco utiliza el sistema SMCD para detectar y desencriptar mensajes sospechosos usando la técnica de cifrado por sustitución simple, la cual va dirigida para prevenir crímenes a nivel global, específicamente ataques terroristas, explosiones de bombas y ataques con drones. El sistema hace uso de diversas bases de datos como TDB, ODB, SSWDB, Metadata y TPDB. El OBIE tiene un papel clave al categorizar las palabras sospechosas en sus respectivos contextos y en el SSWDB se encuentran almacenadas las palabras consideradas sospechosas, mientras que el TPDB compara estas palabras con las palabras base identificadas. Se realizaron las pruebas y se obtuvo como resultado que detectaba las palabras asesinato en un 50% de precisión, palabras de extorsión en 66.66% y en palabras de fraude en un 57.14%, la cual confirma su eficiencia, pero aun así sugieren que este sistema necesita mejorar su precisión.
A2	**Bhan, R., Pamula, R., Faruki, P., & Gajrani, J. (2023)**	Sistema de gestión de confianza basada en blockchain para proteger significativamente a HSN contra ataques internos	Se propone utilizar Hyperledger, una tecnología blockchain, para garantizar la integridad y seguridad de los registros de pacientes y detectar nodos IoMT comprometidos. La blockchain proporciona un registro inmutable y transparente de las transacciones y actividades relacionadas con los datos médicos. La propuesta sugiere el uso del algoritmo ECC para proteger los registros de salud, este es un método criptográfico que proporciona seguridad en la comunicación y asegura que los datos médicos sensibles estén cifrados de forma segura. Se introduce un sistema de confianza jerárquico agrupado (CHTMS) para bloquear y mitigar nodos maliciosos, este sistema contribuye a mantener la integridad y la confianza en la red, bloqueando posibles atacantes y manteniendo la seguridad de los datos de salud.
A3	**Choi, J., Lee, J., & Kim, A. (2023)**	Sistema de "fuzzy vault" (bóveda difusa) de doble clave basado en intervalos de confianza	El objetivo es garantizar la operación confiable de vehículos aéreos no tripulados (UAVs) al anonimizar a los operadores de drones y utilizar de manera segura sus datos y la información a bordo. **Primera Clave (Características únicas del operador):** Esta clave identifica el rostro y el iris, utilizando un intervalo de confianza basándose en una clave generada a partir de la biometría del operador. **Segunda Clave (Lo que el operador recuerda):** Esta clave se utiliza para construir un polinomio y se basa en la memoria del operador, lo que el operador recuerda.
A4	**Subashini, A., & Kanaka Raju, P. (2023).**	sistema de monitorización remota de pacientes para aplicaciones de telemedicina basadas en Internet de las Cosas (IoT)	La técnica se basa en el uso de algoritmos avanzados de inteligencia artificial (IA) para identificar y prever datos de sensores de atención médica Utiliza una mejora de la técnica de ECC para la encriptación, que requiere una longitud de clave más corta y, por lo tanto, reduce el tiempo necesario para encriptar, además se combina con el algoritmo de hash Blake2 para mejorar la seguridad. Emplea un enfoque de criptografía híbrida que combina la encriptación de clave simétrica AES y la encriptación de clave asimétrica ECC.
A5	**Parmar, M., & Shah, P. (2023).**	Mecanismo de criptografía ligera para IoT y blockchain (IBLWC)	La técnica se centra en asegurar la integridad y seguridad de los datos transmitidos desde dispositivos IoT hacia las redes blockchain. **Sincronización de Reloj para Nodos IoT:** Aborda la sincronización de reloj en los nodos IoT que carecen de un mecanismo de reloj interno. Se propone utilizar un protocolo de tiempo de red para sincronizar estos nodos con la red blockchain. **Enfoque Criptográfico Ligero para IoT-Blockchain:** Introduce un enfoque criptográfico ligero, denominado IoT-blockchain light-weight cryptographic (IBLWC), diseñado para asegurar la totalidad del ecosistema IoT-blockchain. Este enfoque busca garantizar la seguridad de los datos que fluyen entre los dispositivos IoT y la red blockchain.

A6	**Yan, J., Lin, W., Tu, X., & Wu, Q. (2023).**	sistema de interacción de productos para hogares inteligentes basado en LoRa (Long Range Radio), dirigido a personas mayores.	Se basa en el uso de algoritmos de intercambio de claves para generar claves secretas compartidas y construir claves de cifrado entre dispositivos terminales. Utiliza un algoritmo de intercambio de claves para generar claves secretas compartidas y construir claves de encriptación entre dispositivos terminales, de esta manera se garantiza la privacidad de los datos informados. Diseña un mecanismo de tolerancia a fallas basado en el teorema de Carmichael para permitir que el centro de control agregue los datos recibidos incluso si hay fallas en los dispositivos terminales o en la conexión de red. Asegura la integridad de los datos informados mediante la verificación en lote, de esta manera ayuda a garantizar que los datos reportados sean íntegros y no hayan sido alterados durante la transmisión.
A7	**Yang, Y.-S., Lee, S.-H., Wang, J.-M., Yang, C.-S., Huang, Y.-M., & Hou, T.-W. (2023).**	Mecanismo de autenticación de identidad basado en criptografía de curva elíptica y tokens	El objetivo es asegurar la seguridad de la transmisión de datos en entornos de IIoT (Internet Industrial de las Cosas) Se propone un mecanismo de autenticación entre los dispositivos terminales IoT y los servidores backend utilizando criptografía de curva elíptica (ECC). Esta técnica se emplea para confirmar la identidad de los dispositivos antes de que se produzca la comunicación. Se utilizan tokens de confianza y encriptación de paquetes mediante el protocolo TLS para garantizar la autenticación y la privacidad en la comunicación entre dispositivos IoT y servidores.
A8	**Nita, S. L., & Mihailescu, M. I. (2023).**	Mecanismo de autenticación para dispositivos IoT basado en curvas elípticas y blockchain	La elección de curvas elípticas se basa en su ligereza, siendo adecuadas para dispositivos IoT con recursos computacionales limitados. También se integra una red blockchain que registra todas las consultas de autenticación mediante contratos inteligentes, el blockchain se comunica con un servidor para validar las consultas de autenticación. Utiliza criptografía de curva elíptica para autenticar dispositivos IoT antes de que puedan enviar datos al servidor de almacenamiento, luego integra una red blockchain para verificar la identidad de los dispositivos que intentan conectarse al sistema para enviar datos al servidor de almacenamiento. Una vez que la identidad se valida en la blockchain, se registra la transacción y se inicia el proceso de transmisión de datos.

A9	**Manzoor, A., Braeken, A., Kanhere, Ylianttila, M., & Liyanage, M. (2021).**	Técnica basada en blockchain y esquemas de re - encriptación de proxy	Esta técnica sirve para garantizar la seguridad y la privacidad de los datos en un entorno de Internet de las cosas (IoT), estos elementos se combinan para abordar la escalabilidad: Se propone utilizar blockchain para crear un mercado descentralizado donde los datos de IoT pueden compartirse de manera segura. Esto elimina la necesidad de un proveedor de servicios centralizado y confiable, así como automatiza los pagos entre las partes involucradas. Se emplea el esquema de reencriptacion proxy para asegurar la transferencia segura y anónima de datos desde el productor de datos al consumidor y así garantizar que solo el propietario y la persona presente en el contrato inteligente puedan visualizar los datos.
A10	**Prakasam, Madheswaran, Sujith, & Sayeed, M. S. (2021)**	Método de criptografía ligera, energéticamente eficiente y mejorada que utiliza manipulación de 8 bits (E3LCM)	El objetivo principal es abordar la necesidad de seguridad en la transmisión de datos en el contexto de IoT y otros sistemas con alta comunicación de datos. El E3LCM se basa en la manipulación de bits de 8 bits, lo que optimiza la eficiencia y el rendimiento del cifrado. Se ha validado utilizando datos de señal de voz y se ha demostrado que consume menos energía y memoria en comparación con otros métodos existentes. Este método criptográfico tiene aplicaciones potenciales en transferencia electrónica de dinero, autenticación y cifrado en aplicaciones de mensajería, entre otros, destacando su capacidad para integrarse en aplicaciones en tiempo real y de alta seguridad, como los entornos IoT.
A11	**Chauhan, C., Ramaiya, M. K., Rajawat, A. S., Goyal, S. B., Verma, C., & Raboaca, M. S. (2022).**	Mecanismo basado en el uso de la tecnología blockchain y la integración de un esquema de cifrado de curvas elípticas.	El objetivo es abordar los desafíos de seguridad y privacidad en el contexto distribuido de Internet de las cosas (IoT) La combinación de criptografía de curva elíptica y tecnología blockchain busca garantizar la seguridad de la información y la autenticación de datos en entornos de IoT, especialmente en ámbitos sensibles como la atención médica. Este enfoque busca proporcionar un mecanismo seguro para compartir y autenticar datos en una amplia variedad de redes y dispositivos heterogéneos que forman parte de IoT.
A12	**Khalifa, M., Algarni, F., Ayoub Khan, M., Ullah, A., & Aloufi, K. (2021)**	Mecanismo centrado en abordar las vulnerabilidades de seguridad asociadas con la recolección de basura (garbage collection) en entornos de Internet of Things (IoT).	El objetivo es proteger la operación del sistema IoT contra ataques de penetración en la memoria heap y la modificación de direcciones. La técnica propuesta implica el cifrado de la recolección de basura de objetos en tiempo de ejecución para prevenir ataques dirigidos y utiliza una función criptográfica hash (Cryptographic Hash Function - CHF) que emplea un algoritmo hash unidireccional específico para formar un mecanismo de firma único. Además, se utiliza una técnica basada en curvas elípticas (ECC) y una clave de un solo uso (OTK) para garantizar la seguridad de la memoria heap.
A13	**Mohammad Shah, I. N., Ismail, E. S., Samat, F., & Nek Abd Rahman, N. (2023)**	Nuevo algoritmo de cifrado ligero que pueda proporcionar un nivel óptimo de seguridad con un número reducido de rondas.	El objetivo es garantizar el transporte, almacenamiento y procesamiento seguro de la gran cantidad de datos privados y sensibles generados por los dispositivos IoT en la red. Específicamente, se propone un nuevo cifrado de bloque ligero basado en una modificación de la estructura de redes Feistel generalizadas (GFN). El enfoque se centra en proporcionar una seguridad óptima con un número reducido de rondas, adaptándose a las limitaciones de recursos de los dispositivos IoT, la estructura GFN es una forma popular de cifrado que divide un mensaje en múltiples subbloques. El algoritmo propuesto fue sometido a análisis estadísticos y criptográficos para evaluar propiedades clave como el efecto avalancha en el cifrado y propiedades aleatorias del algoritmo, luego los resultados demuestran que el algoritmo cumple con los requisitos fundamentales de seguridad para un cifrado de bloque ligero.

A14	**Rana, S., Mondal, M. & Kamruzzaman, J. (2023)**	Cifrado arquitectura de mariposa aleatoria de transformada rápida de Fourier para clave (RBFK)	Proponen una técnica criptográfica llamada "arquitectura de mariposa aleatoria de cifrado de transformada rápida de Fourier para clave" (RBFK) diseñada para abordar los desafíos de seguridad en dispositivos de Internet de las cosas (IoT): El RBFK cipher es un algoritmo de cifrado de clave simétrica diseñado específicamente para dispositivos IoT con recursos limitados, el cifrado RBFK admite dos tamaños de clave diferentes: 64 y 128 bits, lo que permite adaptar la seguridad según las necesidades específicas de la aplicación, además utiliza una arquitectura de mariposa en el sistema de programación de claves para generar claves sólidas para cinco rondas del método de cifrado. Se evaluó el uso de memoria y el ciclo de ejecución del cifrado RBFK utilizando la herramienta de evaluación justa de sistemas criptográficos ligeros (FELICS), lo que demuestra que se llevaron a cabo pruebas para garantizar la eficacia y la eficiencia de la técnica.
A15	**Al Hwaitat, A. K., Almaiah, M. A., Ali, A., Al-Otaibi, S., Shishakly, R., Lutfi, A., & Alrawad, M. (2023)**	Mecanismo de autenticación basado en el cifrado homomórfico	Proponen un nuevo marco de autenticación basado en blockchain diseñado para abordar los desafíos de seguridad y privacidad en aplicaciones de Internet de las cosas (IoT). Se propone utilizar una cadena de bloques (blockchain) basada en permisos para almacenar y verificar las identidades de los dispositivos IoT de manera descentralizada. Esto permite que los dispositivos se autentiquen y se comuniquen de manera segura sin depender de una entidad de confianza central. Se menciona la integración de cifrado homomórfico para cifrar los datos generados por los dispositivos IoT en el extremo del usuario y luego subirlos a la nube. El cifrado homomórfico permite realizar operaciones en los datos cifrados sin necesidad de descifrarlos, lo que mejora la privacidad y la seguridad de los datos.
A16	**Subramaniam, E. V. D., Srinivasan, K., Qaisar, S. M., & Plawiak, P. (2023)**	Cifrado basado en Twine-LiteNet garantizar la confidencialidad de los datos en el Internet de las cosas médicas (IoMT)	Proponen una técnica criptográfica integral para abordar la seguridad en el contexto del Internet de las cosas médicas (IoMT). Se utiliza la autenticación de dispositivos para garantizar que solo dispositivos autorizados tengan acceso a la red de IoT médica. Esto ayuda a prevenir intrusiones no deseadas y garantiza la integridad de la red. Se utiliza el cifrado basado en Twine-LiteNet para garantizar la confidencialidad de los datos transmitidos. Esto es crucial para proteger la privacidad de los datos médicos de los pacientes. Finalmente, los datos cifrados se almacenan de forma segura en un servidor en la nube, lo que garantiza que los datos médicos confidenciales esten protegidos contra accesos no autorizados.

A17	**Rehman, M. U., Shafique, A., & Usman, A. B. (2023)**	Esquema de cifrado de imágenes híbrido basado múltiples técnicas de cifrado en el entorno de IoMT	La técnica propuesta integra múltiples técnicas de cifrado para proteger los datos médicos y garantizar la privacidad del paciente. Cifrado Multietapa: Este cifrado incluye capas de planos de imágenes médicas y utiliza operaciones como rotación, intercambio de filas y columnas, y codificación de ADN para ocultar los datos de la imagen. Cifrado Cuántico: Se incorporan paseos aleatorios cuánticos alternativos como parte del proceso de cifrado, lo que agrega una capa adicional de seguridad basada en principios de mecánica cuántica. Transformación del Cubo de Rubik: consiste en introducir un nivel de caos en el proceso de cifrado, dificultando la decodificación no autorizada. Criptosistema de Curva Elíptica con Hill Cipher (ECCHC): Esta técnica se integra en el proceso de cifrado para proporcionar una capa adicional de seguridad basada en criptografía de curva elíptica y el cifrado de Hill. Mutación de ADN: El esquema incluye la mutación del ADN, lo que agrega complejidad y hace que el cifrado sea más resistente a ataques.
A18	**Román, R., Arjona, R., & Baturone, I. (2023)**	Mecanismos certificación remota basadas en hash para dispositivos IoT de gama baja	La técnica utiliza firmas digitales basadas en hash en el protocolo de certificación y además estas firmas son robustas y resistentes a los ataques cuánticos, lo que garantiza la seguridad de la certificación. El protocolo de certificación aprovecha el uso de firmas única (OTS) y verificación de firma múltiple (MTS) que son adecuadas para dispositivos de recursos limitados como los dispositivos IoT. Estos esquemas son eficientes en términos de tamaño de código y tiempos de ejecución.
A19	**Sahoo, S., Mohanty, S., Sahoo, K., Daneshmand, M., & Gandomi, A. H. (2023**	Esquema de autenticación de tres factores (TDTAS) basado en criptografía de curva elíptica (ECC)	El objetivo principal de esta técnica es garantizar la seguridad de la transmisión de datos entre dispositivos IoT en una red 5G. El esquema TDTAS utiliza tres factores de autenticación para fortalecer la seguridad: algo que el usuario conoce (contraseña), algo que el usuario posee (dispositivo IoT), y algo que el usuario es (identidad biométrica o característica física).

A20	**Sahoo, S., Mohanty, S., Sahoo, K., Daneshmand, M., & Gandomi, A. H. (2023)**	Sistema de cifrado logístico híbrido basado en ADN para proteger sistema de monitorización en entornos de IoMT	El objetivo de esta técnica criptográfica es mejorar la seguridad en la transmisión de datos médicos en el contexto de Internet de las cosas (IoT). Para lograrlo se utilizan técnicas de cifrado avanzadas como el cifrado AES y la caótica de ADN para garantizar una alta seguridad contra ataques falsificados de IoT. Lo distintivo de esta técnica es la combinación de estas técnicas mencionadas, los mapas caóticos 3D se utilizan para agregar una capa adicional de aleatoriedad y complejidad al proceso de cifrado para aumentar la seguridad. Según los resultados experimentales, se demuestra que la técnica de cifrada propuesta supera a otros métodos competidores y es especialmente adecuada para establecer un alto nivel de seguridad en la transmisión de datos médicos.
A21	**Ali, U., Idris, M. Y. I. B., Frnda, J., Ayub, M. N. B., Khan, M. A., Khan, N., Beegum T, R., Jasim, A. A., Ullah, I., & Babar, M. (2023)**	Esquema de cifrado autenticado con datos asociados (AEAD) y criptografía de curva elíptica (ECC) basado en el esquema de autenticación sin certificado seguro y ligero mejorado (ELWSCAS)	Proponen la implementación de un sistema de seguridad para entornos de IoT que cumpla con los requisitos de seguridad y rendimiento liviano necesarios. Esta técnica incluye el uso de un cifrado autenticado con datos asociados (AEAD) y la criptografía de curva elíptica (ECC), basado en el esquema de autenticación sin certificado seguro y ligero mejorado (ELWSCAS). Se destaca que la técnica propuesta es eficiente en términos de cómputo y comunicación. En comparación con enfoques existentes, se afirma que la técnica es considerablemente menos costosa y adecuada para entornos de IoT con recursos limitados.
A22	**Vaidya, S., Suri, A., Batla, V., Keshta, I., Ajibade, S.-S. M., & Safarov, G. (2023).**	Esquema de cifrado basado en funciones con una estructura de acceso oculta para la seguridad de los datos médicos de IoT	Propone una técnica que convierte el Cifrado Basado en la Identidad (IBE) en modelo de cifrado basado en características (FBEM) con atributos multivalor y puerta. El artículo recomienda un modelo de cifrado basado en características (FBEM) como técnica criptográfica, este permite un control fino del acceso a los datos cifrados y garantiza la privacidad de los datos médicos del paciente. Acceso Granular y Control de Acceso: El objetivo principal es establecer un control de acceso detallado sobre los datos cifrados, lo que significa que solo usuarios autorizados pueden acceder a datos específicos según sus atributos o características. Conversión de IBE a FBEM: Se utiliza una técnica de conversión universal para transformar un sistema de IBE en un modelo FBEM que admite atributos multi-valor y puertas lógicas. Esto permite heredar las características de IBE en el nuevo modelo FBEM. Acceso Estructura Oculta: El FBEM se utiliza para construir un escenario de IoT médico, y se destaca que la estructura de acceso se oculta en este proceso. Esto significa que, incluso si alguien accede al cifrado, no puede comprender la estructura de acceso. El artículo afirma que la técnica propuesta ofrece ventajas en eficiencia computacional, carga de almacenamiento y seguridad en comparación con sistemas prominentes cuando la estructura de acceso está oculta.

A23	**Ramyasri, G., Murthy, G. R., Itapu, S., & Krishna, S. M. (2023).**	Mecanismo de criptografía de curva elíptica (ECC) para cifrar y proteger los datos durante su transferencia en un entorno de IoT a través del protocolo MQTT	El objetivo de esta técnica es proteger la transferencia de datos desde el extremo del publicador (dispositivo emisor) hasta el extremo del suscriptor (dispositivo receptor). El protocolo MQTT se utiliza para facilitar la transferencia de datos entre los componentes del sistema IoT, lo que incluye la publicación y la suscripción a mensajes. Para garantizar la seguridad de las comunicaciones, se implementa la criptografía de clave pública basada en ECC. Este enfoque utiliza una clave pública y una clave privada para cifrar y descifrar los datos transmitidos. Cuando los datos se envían desde un dispositivo Raspberry Pi (o cualquier dispositivo publicador), se cifran utilizando ECC antes de ser transmitidos a través del protocolo MQTT al broker o servicio de suscripción y en el extremo del suscriptor, los datos cifrados se descifran utilizando la clave privada correspondiente. El artículo señala que la combinación de ECC y MQTT demostró ser eficiente tanto para transmisiones de datos en modo ráfaga como para transmisiones continuas, en comparación con las técnicas criptográficas convencionales.
A24	**Shilpa, Vidya, & Pattar, S. (2022)**	Mejora del protocolo MQTT mediante la implementación de autenticación mutua y cifrado de datos ligero	Proponen el protocolo SEC-RMC, que usa Mosquitto MQTT en dispositivos IoT para lograr comunicación segura y eficiente. El protocolo utiliza un algoritmo de cifrado ligero para proteger las comunicaciones entre dispositivos IoT. Este cifrado garantiza que los datos transmitidos sean seguros y no puedan ser interceptados o alterados por terceros no autorizados. El protocolo SEC-RMC proporciona autenticación mutua, lo que significa que tanto los dispositivos emisores como los receptores se autentican entre sí antes de permitir la comunicación. Esto garantiza que los dispositivos se reconozcan mutuamente como legítimos y no se produzcan comunicaciones no autorizadas. El artículo afirma que el esquema propuesto reduce significativamente el número de mensajes transmitidos entre los dispositivos, lo que contribuye a una comunicación más eficiente. Además, se menciona que se logra una reducción del 80% en el tiempo de transmisión en comparación con métodos existentes.
A25	**Masud, M., Gaba, G. S., Kumar, P., & Gurtov, A. (2022)**	Protocolo de autenticación centrado en el usuario que preserva la privacidad para entornos IoT-AmI	El artículo propone una técnica criptográfica para mejorar la seguridad en las aplicaciones de atención médica basadas en Ambient Intelligence (AmI) en Internet de las cosas (IoT). El protocolo implementa un mecanismo de autenticación de dispositivos que utiliza técnicas como funciones físicamente no clonables (PUF) y biometría para verificar la identidad de los dispositivos. Esto previene ataques de suplantación, ataques de repetición y ataques de clonación. En lugar de depender de la criptografía de clave pública convencional y multiplicaciones escalares, el protocolo utiliza primitivas criptográficas livianas como funciones de hash y PUF. Esto ayuda a reducir la complejidad computacional y los recursos necesarios para la autenticación. El protocolo se diseñó para ser eficiente en cuanto a recursos, lo que significa que utiliza un consumo mínimo de recursos computacionales y de ancho de banda.

A26	**Shukla, S., Thakur, S., Hussain, S., Breslin, J. G., & Jameel, S. M. (2021)**	Modelo de cadena de bloques basado en computación de niebla integrada para la Identificación y autenticación en el Internet de las cosas de atención médica (LoMT)	El artículo propone una técnica criptográfica para abordar la seguridad en dispositivos de Internet de las cosas (IoT) en el entorno de la atención médica. Se introduce el algoritmo ASE (Advanced Signature-Based Encryption) para la identificación de dispositivos de IoT, la verificación y la autenticación de los Datos de Salud del Paciente (PHD). Este algoritmo se utiliza para garantizar la seguridad de la transmisión de datos y la detección de nodos maliciosos. Los resultados de rendimiento muestran que el algoritmo ASE en el entorno de Fog Computing supera a otras técnicas y arquitecturas existentes en términos de detección de nodos maliciosos, confiabilidad y precisión de transmisión de datos.
A27	**Margelis, G., Fafoutis, X., Oikonomou, G., Piechocki, R., Tryfonas, T., & Thomas, P. (2019).**	Esquema de generación de claves secretas	Proponen una técnica criptográfica llamada SKYGlow para abordar la seguridad en dispositivos de Internet de las cosas (IoT) que tienen limitaciones de recursos y no pueden emplear esquemas tradicionales de distribución de claves. La criptografía SKYGlow se centra en la generación de claves secretas en dispositivos IoT directamente desde la información compartida en el canal de comunicación sin necesidad de una distribución centralizada de claves. Esto permite a los dispositivos IoT generar claves de cifrado secretas sin depender de una infraestructura central. SKYGlow también utiliza la Transformada de Coseno Discreto (DCT) en observaciones del canal de mensajes intercambiados entre dispositivos IoT. Esta técnica reduce las discrepancias y aumenta la correlación entre los bits secretos generados, lo que mejora la calidad de las claves secretas. El artículo presenta pruebas realizadas en escenarios tanto en interiores como en exteriores, utilizando radios IEEE 802.15.4 a diferentes frecuencias (2.4 GHz y 868 MHz) y los resultados indican que SKYGlow puede generar claves secretas de 128 bits con alta entropía a partir de 65 intercambios de paquetes, lo que demuestra su eficiencia energética y su capacidad para superar las técnicas existentes en términos de rendimiento.
A28	**Aishwariya, R. & Arunachalam, A. (2023)**	Enfoque de detección de malware y mejora en la seguridad de dispositivos LoT basados en criptografía de curva elíptica mejorada (IECC)	Proponen un enfoque basado en criptografía de curva elíptica junto a un modelo de aprendizaje profundo, como Deep LSTM, para la detección de malware y garantizar la seguridad de los datos durante su transmisión. Después de la detección de malware, se implementa la prevención utilizando el algoritmo Improved Elliptic Curve Cryptography (IECC), luego se utiliza una optimización híbrida MA-BW para seleccionar la clave óptima durante la transmisión de datos. Se realizan pruebas de rendimiento utilizando Python 3.8 y se comparan con varias técnicas existentes logrando una precisión del 95%, un valor de error del 5% y una precisión del 92%. Además, el algoritmo Improved ECC se compara con otros algoritmos existentes y resulta que tiene un mejor rendimiento y una mejor seguridad para los dispositivos IoT durante la transmisión de datos.

Discusiones

Como nos podemos haber dado cuenta el uso de la criptografía es muy útil pero también altamente complejo al utilizarlo, nuestra investigación revela una diversidad de técnicas criptográficas muy efectivas como también algunas que no son tan efectivas, pero todas abordan desafíos cruciales de seguridad y privacidad en entornos IoT. Todas las técnicas que se evaluaron se analizó que usaron 3 principales algoritmos de encriptación que son de cifrado público el AES y de cifrado privado el EEC y las funciones Hash y además utilizan con mucha frecuencia la tecnología de blockchain para fortalecer la seguridad de datos y por ende hacerla más compleja el descifrado.

En el ámbito de la salud, el ECC se implementa en un Sistema de Gestión de Confianza basada en blockchain. Este sistema protege contra ataques internos en entornos de Health Information Systems (HSN) (Bhan et al., 2023). Además, se aplica en un Sistema de Monitorización Remota de Pacientes para aplicaciones de telemedicina basadas en IoT, mejorando la eficiencia de la encriptación y reduciendo la longitud de la clave necesaria (Subashini et al., 2023). También se utiliza en un Mecanismo de Autenticación de Identidad basado en criptografía de curva elíptica y tokens, confirmando la identidad de dispositivos IoT antes de la comunicación (Yang et al., 2023). Otro uso relevante es en un Mecanismo de Autenticación para

Dispositivos IoT basado en curvas elípticas y blockchain, utilizado para autenticar dispositivos antes de enviar datos al servidor de almacenamiento (Nita et al., 2023).

En otros contextos, el ECC se implementa en un Mecanismo basado en tecnología blockchain y cifrado de curvas elípticas para proporcionar un mecanismo seguro para compartir y autenticar datos en redes y dispositivos heterogéneos (Chauhan et al., 2022). También se aplica en un Mecanismo centrado en abordar las vulnerabilidades de seguridad en la recolección de basura en IoT, garantizando la seguridad de la memoria heap y protegiendo contra ataques en tiempo de ejecución (Khalifa et al., 2021). Otros usos incluyen un Esquema de Cifrado de Imágenes Híbrido en IoMT, un Esquema de Autenticación de Tres Factores y un Esquema de Cifrado Autenticado con Datos Asociados (Rehman et al., 2023; Swagatika et al., 2023; Ali et al., 2023). Además, se emplea en un Mecanismo de Transferencia Segura de Datos en entornos IoT a través de MQTT, cifrando los datos antes de ser transmitidos (Ramyasri et al., 2023). Finalmente, el ECC se utiliza junto con un modelo de aprendizaje profundo en un Mecanismo para la Detección de Malware y Mejora de la Seguridad en Dispositivos IoT (Aishwariya et al., 2023).

También se observó que las soluciones criptográficas analizadas en el estudio utilizan el algoritmo estándar de cifrado avanzado (AES), ya sea de forma independiente o combinado con otros algoritmos. Esta técnica de cifrado se aplica en varias soluciones criptográficas, como el Sistema de cifrado logístico híbrido basado en ADN para IoMT (Ettiyan et al., 2023), donde se utiliza el cifrado AES para mejorar la seguridad en la transmisión de datos médicos en el contexto de IoT. En el caso de la detección de malware y mejora de la seguridad en dispositivos IoT (Aishwariya et al., 2023), el algoritmo AES se utiliza como parte de la prevención después de la detección de malware en un enfoque basado en IECC y Deep LSTM. Asimismo, el Sistema de monitorización remota de pacientes para IoT (Subashini et al., 2023) emplea el algoritmo AES para fortalecer la seguridad, combinándolo con la criptografía EEC como parte de un enfoque híbrido. Además, en el modelo de cadena de bloques basado en computación de niebla integrada para el Internet de las cosas en atención médica (Shukla et al., 2021), se introduce el algoritmo AES para garantizar la seguridad en la transmisión de datos y la detección de nodos maliciosos.

Además, se identificaron tres soluciones criptográficas que incorporan funciones hash en su arquitectura. La primera es un mecanismo de certificación remota para dispositivos IoT de gama baja (Román et al., 2023), que emplea firmas digitales basadas en hash para la certificación remota. La segunda solución es un protocolo de autenticación centrado en el usuario para entornos IoT-AmI (Masud et al., 2023), donde las funciones de hash son parte integral del protocolo de autenticación centrado en el usuario. La tercera solución es un esquema de generación de claves secretas (Margelis et al., 2019), que se centra en generar claves secretas en dispositivos IoT directamente desde la información compartida en el canal de comunicación, sin depender de una distribución centralizada de claves. Estos hallazgos resaltan la importancia de los algoritmos hash en la garantía de seguridad, integridad de datos, eficiencia computacional y autenticación de firmas digitales en dispositivos IoT.

Por otro lado, aparte de los algoritmos de encriptación, se destaca la importancia de la tecnología blockchain en varias soluciones criptográficas revisadas. Entre ellas, el Sistema de Detección de Mensajes Criptográficos Sospechosos (Hussain et al., 2023) utiliza un marco basado en blockchain para detectar y desencriptar mensajes sospechosos, ofreciendo una capa adicional de seguridad y transparencia en el proceso de detección. El Sistema de Gestión de Confianza (Bhan et al., 2023) actúa como un registro inmutable y transparente, asegurando la confiabilidad y seguridad de los datos médicos. En el Sistema de Monitorización Remota de Pacientes para IoT (Subashini et al., 2023), la blockchain se combina con criptografía de curva elíptica y AES en un enfoque híbrido, contribuyendo a la seguridad y transparencia de la red. El Mecanismo de Criptografía Ligera para IoT (Parmar et al., 2023) se posiciona como la piedra angular para garantizar la confianza e integridad de los datos en el entorno IoT. Además, la técnica basada en blockchain y esquemas de encriptación de proxy (Manzoor et al., 2021) proporciona seguridad y transparencia en la transferencia de datos entre productores y consumidores. El Mecanismo de Autenticación basado en el cifrado homomórfico

(Hwaita et al., 2023) utiliza esta tecnología para almacenar y verificar identidades descentralizadas de dispositivos IoT, mientras que el cifrado homomórfico cifra datos antes de cargarlos en la nube. Estos ejemplos resaltan la relevancia de la tecnología blockchain en garantizar seguridad, integridad y transparencia en diversos escenarios de aplicaciones criptográficas.

Conclusión

En la era digital actual, la seguridad de la información es de suma importancia, especialmente en entornos como el Internet de las Cosas (IoT) donde la interconexión de dispositivos y la transferencia de datos sensibles son omnipresentes, en por ello que en esta revisión sistemática se concluye que las principales técnicas de criptografía aplicadas en entornos de IOT son la criptografía de curva elíptica (ECC), el estándar de encriptación avanzada(AES) y las funciones hash, estas técnicas se ha identificado avances significativos en esta era digital.

La criptografía de curva elíptica (ECC), es utilizada como una técnica integral para fortalecer la seguridad especialmente en aplicaciones IoT que tienen pocos recursos. Su eficiencia radica en ofrecer un alto nivel de seguridad con claves más pequeñas en comparación con otros algoritmos de cifrado como RSA, crucial para dispositivos IoT con recursos limitados. Además, la ECC presenta una notable resistencia contra ataques comunes, como la factorización de claves, proporcionando una protección sólida de la información. Su adaptabilidad la hace versátil y fácil de implementar en diversas plataformas, además se puede incorporar con enfoques de aprendizaje profundo para mejorar significativamente la detección de malware y la seguridad de la información durante la transmisión de datos.

El Estándar de Encriptación Avanzada (AES) se muestra como técnica altamente efectiva para garantizar la seguridad en la transmisión de datos, especialmente en aplicaciones críticas como la atención médica. Su fortaleza reside en ofrecer un nivel excepcional de seguridad sin comprometer la eficiencia, además se posiciona como un marco sólido para la confiabilidad de las comunicaciones en entornos IoT. Por consiguiente, este algoritmo ha sido sometido a muchas pruebas en muchas investigaciones, en los cuales se mostró su alta efectividad ante diversos ataques en entornos IoT.

Finalmente afirmamos que la función hash criptográfica es muy útil en términos de seguridad en entornos IoT, utilizándose como un complemento en infraestructuras ECC, AES entre otros, debido a que asegura la integridad de la información al generar un resumen único para conjuntos de datos, desempeñando un papel crucial en la autenticación. En comparación con otros mecanismos de autenticación de datos en entornos IoT, este enfoque reduce la carga computacional garantizando eficiencia en la verificación de datos críticos, especialmente en entornos IoT donde la rapidez y precisión son muy necesarios.

En cuanto a las líneas de investigación futura, proponemos la exploración de enfoques avanzados como el cifrado cuántico, debido a su reciente descubrimiento, existe un limitado número de estudios sobre sus avances en términos de seguridad de la información, también proponemos la integración de aprendizaje automático en diversas técnicas de cifrado, con el objetivo de potenciar la detección y prevención de amenazas en tiempo real en entornos de IoT. Estas investigaciones no solo contribuirán al avance del conocimiento en seguridad, sino que también ofrecerán perspectivas innovadoras para enfrentar los desafíos emergentes en la protección de datos en entornos interconectados.

Referencias bibliográficas

Abdur, M., Habib, S., Ali, M., & Ullah, S. (2017). Security issues in the internet of things (IoT): A comprehensive study. *International Journal of Advanced Computer Science and Applications*#: IJACSA, 8(6). https://doi.org/10.14569/ijacsa.2017.080650

Aiyshwariya Devi, R., & Arunachalam, A. R. (2023). Enhancement of IoT device security using an Improved Elliptic Curve Cryptography algorithm and malware detection utilizing deep LSTM. *High-Confidence Computing*, 3(2), 100117. https://doi.org/10.1016/j.hcc.2023.100117

Al Hwaitat, A. K., Almaiah, M. A., Ali, A., Al-Otaibi, S., Shishakly, R., Lutfi, A., & Alrawad, M. (2023). A new blockchain-based authentication framework for secure IoT networks. Electronics, 12(17), 3618. https://doi.org/10.3390/electronics12173618

Ali, U., Idris, M. Y. I. B., Frnda, J., Ayub, M. N. B., Khan, M. A., Khan, N., Beegum T, R., Jasim, A. A., Ullah, I., & Babar, M. (2023). Enhanced lightweight and secure certificateless authentication scheme (ELWSCAS) for Internet of Things environment. *Internet of Things*, 24(100923), 100923. https://doi.org/10.1016/j.iot.2023.100923

Bhan, R., Pamula, R., Faruki, P., & Gajrani, J. (2023). Blockchain-enabled secure and efficient data sharing scheme for trust management in healthcare smartphone network. *The Journal of Supercomputing*, 79(14), 16233–16274. https://doi.org/10.1007/s11227-023-05272-6

Bhatt, A. P., & Sharma, A. (2019). Quantum Cryptography for Internet of Things Security. *Journal of Electronic Science and Technology*, 17(3), 213-220. https://doi.org/10.11989/JEST.1674-862X.90523016

Caraveo-Cacep, M. A., Vázquez-Medina, R., & Hernández Zavala, A. (2023). A survey on low-cost development boards for applying cryptography in IoT systems. *Internet of Things*, 22(100743), 100743. https://doi.org/10.1016/j.iot.2023.100743

Chauhan, C., Ramaiya, M. K., Rajawat, A. S., Goyal, S. B., Verma, C., & Raboaca, M. S. (2022). Improving IoT security using elliptic curve integrated encryption scheme with primary structure-based block chain technology. *Procedia Computer Science*, 215, 488–498. https://doi.org/10.1016/j.procs.2022.12.051

Choi, J., Lee, J., & Kim, A. (2023). An efficient confidence interval-based dual-key fuzzy vault scheme for operator authentication of autonomous unmanned aerial vehicles. *Applied Sciences*, 13(15), 8894. https://doi.org/10.3390/app13158894

Ettiyan, R., & Geetha. (2023). A hybrid logistic DNA-based encryption system for securing the Internet of Things patient monitoring systems. *Healthcare Analytics*, 3(100149), 100149. https://doi.org/10.1016/j.health.2023.100149

Huo, X., & Wang, X. (2023). Internet of things for smart manufacturing based on advanced encryption standard (AES) algorithm with chaotic system. *Results in Engineering*, 20(101589), 101589. https://doi.org/10.1016/j.rineng.2023.101589

Hussain, S., & Mohideen S, P. (2023). SCMD suspicious cryptographic message detection. *Measurement:Sensors*, 29(100863), 100863. https://doi.org/10.1016/j.measen.2023.100863

Índice de Inteligencia de Amenazas de IBM Security X-Force de 2023. (2023). Ibm.com. Recuperado el 28 de noviembre de 2023, de https://www.ibm.com/es-es/reports/threat-intelligence

Khalifa, M., Algarni, F., Ayoub Khan, M., Ullah, A., & Aloufi, K. (2021). A lightweight cryptography (LWC) framework to secure memory heap in Internet of Things. *Alexandria Engineering Journal*, 60(1), 1489–1497. https://doi.org/10.1016/j.aej.2020.11.003

Liestyowati, D. (2020). Public Key Cryptography. Journal of physics. *Conference series*, 1477(5), 052062. https://doi.org/10.1088/1742-6596/1477/5/052062

Manzoor, A., Braeken, A., Kanhere, Ylianttila, M., & Liyanage, M. (2021). Proxy re-encryption enabled secure and anonymous IoT data sharing platform based on blockchain. *Journal of Network and Computer Applications*, 176(102917), 102917. https://doi.org/10.1016/j.jnca.2020.102917

Margelis, G., Fafoutis, X., Oikonomou, G., Piechocki, R., Tryfonas, T., & Thomas, P. (2019). Efficient DCT-based secret key generation for the Internet of Things. *Ad Hoc Networks*, 92(101744), 101744. https://doi.org/10.1016/j.adhoc.2018.08.014

Martínez-Santander, C. J., & Cruz-Gavilánez, Y. de la N. (2018). Tendencias tecnológicas y desafíos de la seguridad informática. *Polo del Conocimiento*, 3(5), 260. https://doi.org/10.23857/pc.v3i5.640

Masud, M., Gaba, G. S., Kumar, P., & Gurtov, A. (2022). A user-centric privacy-preserving authentication protocol for IoT-AmI environments. Computer Communications, 196, 45–54. https://doi.org/10.1016/j.comcom.2022.09.021

Mohammad Shah, I. N., Ismail, E. S., Samat, F., & Nek Abd Rahman, N. (2023). Modified generalized Feistel network block cipher for the Internet of Things. *Symmetry*, 15(4), 900. https://doi.org/10.3390/sym15040900

Nita, S. L., & Mihailescu, M. I. (2023). Elliptic curve-based query authentication protocol for IoT devices aided by blockchain. Sensors (Basel, Switzerland), 23(3), 1371. https://doi.org/10.3390/s23031371

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., ... Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *Journal of Clinical Epidemiology*, 134, 178–189. https://doi.org/10.1016/j.jclinepi.2021.03.001

Parmar, M., & Shah, P. (2023). Internet of things-blockchain lightweight cryptography to data security and integrity for intelligent application. *International Journal of Electrical and Computer Engineering* (IJECE), 13(4), 4422. https://doi.org/10.11591/ijece.v13i4.pp4422-4431

Prakasam, Madheswaran, Sujith, & Sayeed, M. S. (2021). An Enhanced Energy Efficient Lightweight Cryptography Method for various IoT devices. *ICT Express*, 7(4), 487–492. https://doi.org/10.1016/j.icte.2021.03.007

Ramyasri, G., Ramana Murthy, G., Itapu, S., & Mohan Krishna, S. (2023). Data transmission using secure hybrid techniques for smart energy metering devices. *E-Prime - Advances in Electrical Engineering, Electronics and Energy*, 4(100134), 100134. https://doi.org/10.1016/j.prime.2023.100134

Rana, S., Mondal, M. & Kamruzzaman, J. (2023). RBFK cipher: a randomized butterfly architecture-based lightweight block cipher for IoT devices in the edge computing environment. *Cybersecurity*, 6(1). https://doi.org/10.1186/s42400-022-00136-7

Rehman, M. U., Shafique, A., & Usman, A. B. (2023). Securing medical information transmission between IoT devices: An innovative hybrid encryption scheme based on quantum walk, DNA encoding, and chaos. *Internet of Things*, 24(100891), 100891. https://doi.org/10.1016/j.iot.2023.100891

Román, R., Arjona, R., & Baturone, I. (2023). A lightweight remote attestation using PUFs and hash-based signatures for low-end IoT devices. *Future Generations Computer Systems: FGCS*, 148, 425–435. https://doi.org/10.1016/j.future.2023.06.008

Sahoo, S., Mohanty, S., Sahoo, K., Daneshmand, M., & Gandomi, A. H. (2023). A three-factor-based authentication scheme of 5G wireless sensor networks for IoT system. *IEEE internet of things journal*, 10(17), 15087–15099. https://doi.org/10.1109/jiot.2023.3264565

Shilpa, Vidya, & Pattar, S. (2022). MQTT based secure transport layer communication for mutual authentication in IoT network. *Global Transitions Proceedings*, 3(1), 60–66. https://doi.org/10.1016/j.gltp.2022.04.015

Shukla, S., Thakur, S., Hussain, S., Breslin, J. G., & Jameel, S. M. (2021). Identification and authentication in healthcare internet-of-things using integrated fog computing based blockchain model. *Internet of Things*, 15(100422), 100422. https://doi.org/10.1016/j.iot.2021.100422

Subashini, A., & Kanaka Raju, P. (2023). Hybrid AES model with elliptic curve and ID based key generation for IOT in telemedicine. *Measurement: Sensors*, 28(100824), 100824. https://doi.org/10.1016/j.measen.2023.100824

Subramaniam, E. V. D., Srinivasan, K., Qaisar, S. M., & Pławiak, P. (2023). Interoperable IoMT approach for remote diagnosis with privacy-preservation perspective in edge systems. *Sensors*, 23(17), 7474. https://doi.org/10.3390/s23177474

Tezcan, C. (2022). Key lengths revisited: GPU-based brute force cryptanalysis of DES, 3DES, and PRESENT. *Journal of Systems Architecture*, 124(102402), 102402. https://doi.org/10.1016/j.sysarc.2022.102402

Ullah, F., & Pun, C.-M. (2023). Deep self-learning based dynamic secret key generation for novel secure and efficient hashing algorithm. *Information Sciences*, 629, 488–501. https://doi.org/10.1016/j.ins.2023.02.007

Vaidya, S., Suri, A., Batla, V., Keshta, I., Ajibade, S.-S. M., & Safarov, G. (2023). A computer-aided feature-based encryption model with concealed access structure for medical Internet of Things. *Decision Analytics Journal*, 7(100257), 100257. https://doi.org/10.1016/j.dajour.2023.100257

Yan, J., Lin, W., Tu, X., & Wu, Q. (2023). IoT-based interaction design of smart home products for elderly families. *Applied Mathematics and Nonlinear Sciences*. https://doi.org/10.2478/amns.2023.1.00196

Yang, Y.-S., Lee, S.-H., Wang, J.-M., Yang, C.-S., Huang, Y.-M., & Hou, T.-W. (2023). Lightweight authentication mechanism for industrial IoT environment combining elliptic curve cryptography and trusted token. *Sensors*, 23(10), 4970. https://doi.org/10.3390/s23104970