UNIVERSIDAD POLITÉCNICA SALESIANA

SEDE QUITO

CARRERA DE TELECOMUNICACIONES

ANÁLISIS DEL IMPACTO DE LA COMPUTACIÓN CUÁNTICA EN LA SEGURIDAD DE LAS REDES DE INTERNET DE LAS COSAS IOT.

Trabajo de titulación previo a la obtención del
Título de Ingeniero en Telecomunicaciones

AUTORES: Edison Joel Chuqui Jaya
Alex Dario Lugmaña Huacho.
TUTOR: Juan Carlos Domínguez Ayala.

Quito-Ecuador
2025

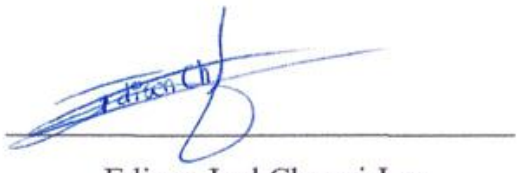
CERTIFICADO DE RESPONSABILIDAD Y AUTORÍA DEL TRABAJO DE TITULACIÓN

Nosotros, Edison Joel Chuqui Jaya con documento de identificación N° 1725029464 y Alex Dario Lugmaña Huacho con documento de identificación N° 1724216310; manifestamos que:

Somos los autores y responsables del presente trabajo; y, autorizamos a que sin fines de lucro la Universidad Politécnica Salesiana pueda usar, difundir, reproducir o publicar de manera total o parcial el presente trabajo de titulación.

Quito, 10 de febrero del año 2025

Atentamente,



Edison Joel Chuqui Jaya
1725029464

Alex Dario Lugmaña Huacho
1724216310

CERTIFICADO DE CESIÓN DE DERECHOS DE AUTOR DEL TRABAJO DE TITULACIÓN A LA UNIVERSIDAD POLITÉCNICA SALESIANA

Nosotros, Edison Joel Chuqui Jaya con documento de identificación N° 1725029464 y Alex Dario Lugmaña Huacho con documento de identificación N° 1724216310, expresamos nuestra voluntad y por medio del presente documento cedo a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que somos autores del Artículo Académico: "Análisis del impacto de la computación cuántica en la seguridad de las redes de internet de las cosas IoT.", el cual ha sido desarrollado para optar por el título de: Ingeniero en Telecomunicaciones, en la Universidad Politécnica Salesiana, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En concordancia con lo manifestado, suscribo este documento en el momento que hago la entrega del trabajo final en formato digital a la Biblioteca de la Universidad Politécnica Salesiana.

Quito, 10 de febrero del año 2025

Atentamente,

Edison Joel Chuqui Jaya
1725029464

Alex Dario Lugmaña Huacho
1724216310

CERTIFICADO DE DIRECCIÓN DEL TRABAJO DE TITULACIÓN

Yo, Juan Carlos Domínguez Ayala con documento de identificación N° 1713195590, docente de la Universidad Politécnica Salesiana, declaro que bajo mi tutoría fue desarrollado el trabajo de titulación: ANÁLISIS DEL IMPACTO DE LA COMPUTACIÓN CUÁNTICA EN LA SEGURIDAD DE LAS REDES DE INTERNET DE LAS COSAS IOT, realizado por Edison Joel Chuqui Jaya con documento de identificación N° 1725029464 y Alex Dario Lugmaña Huacho con documento de identificación N° 1724216310 obteniendo como resultado final el trabajo de titulación bajo la opción de artículo académico que cumple con todos los requisitos determinados por la Universidad Politécnica Salesiana.

Quito, 10 de febrero del año 2025

Atentamente,

Ing. Juan Carlos Dominguez Ayala, MSc
1713195590

DEDICATORIA

Dedico este trabajo de titulación a mis padres Rodrigo y Teresa, y hermanos por su amor, sacrificio y apoyo incondicional. Gracias por creer en mí en cada paso de este largo camino. A Dios, por darme la fuerza, la paciencia y la sabiduría para llegar hasta aquí. Gracias por guiar mis pasos y por brindarme la paz que necesito en cada momento. Y a mis compañeros, por su compañía, por sus palabras de aliento y por recordarme que, en los momentos de duda, nunca estoy solo. Esta es una victoria compartida con todos ustedes.

Edison Chuqui

Dedico este trabajo a mis padres, por su apoyo constante, su esfuerzo y los valores que me han transmitido a lo largo de los años. A mi hermano, por su acompañamiento y solidaridad. Esta dedicatoria es un reconocimiento a su presencia fundamental en mi vida y al impacto que cada uno de ustedes ha tenido en mi crecimiento personal.

Alex Lugmaña

.

AGRADECIMIENTO

Quiero expresar mi más sincero agradecimiento a la Universidad Politécnica Salesiana, por brindarnos las herramientas necesarias para alcanzar este logro. A los profesores y al personal académico, por su dedicación, apoyo y por enseñarnos a cuestionar, investigar y aprender con pasión.

A mi familia, por su amor incondicional, por creer en mí incluso cuando las dudas eran muchas. A ustedes les debo todo, ya que siempre me han impulsado a dar lo mejor de mí en cada paso de mi vida. Gracias por su paciencia, su comprensión y por estar a mi lado en cada momento de este proceso.

A mis compañeros, quienes compartieron este camino y lo hicieron mucho más llevadero. Sus consejos, risas y momentos de apoyo fueron fundamentales para continuar cuando el camino parecía incierto. Cada uno de ustedes contribuyó a mi crecimiento.

Edison Chuqui y Alex Lugmaña

ANÁLISIS DEL IMPACTO DE LA COMPUTACIÓN CUÁNTICA EN LA SEGURIDAD DE LAS REDES DE INTERNET DE LAS COSAS IOT.

ANALYSIS OF THE IMPACT OF QUANTUM QUANTUM COMPUTING ON THE SECURITY OF INTERNET OF THINGS IOT NETWORKS INTERNET OF THINGS IOT NETWORKS.

Edison Joel Chuqui Jaya[1], , Alex Dario Lugmaña Huacho[2], , Juan Carlos Domínguez Ayala[1],

Resumen

El artículo analiza el impacto de la computación cuántica en la seguridad de las redes de Internet de las Cosas (IoT). Explica cómo la computación cuántica, mediante algoritmos como Shor y Grover, representa una amenaza para los sistemas de cifrado actuales, como RSA y ECC, utilizados en la protección de datos IoT. También examina vulnerabilidades en protocolos de seguridad y presenta soluciones emergentes, como la criptografía post-cuántica y la distribución cuántica de claves (QKD). Finalmente, se destacan estrategias para mitigar riesgos, incluyendo la integración de inteligencia artificial, 5G y redes cuánticas seguras en la infraestructura IoT.

Palabras clave: Iot, RSA, ECC, Criptografica post-cuántica.

Abstract

The article discusses the impact of quantum computing on the security of Internet of Things (IoT) networks. He explains how quantum computing, using algorithms such as Shor and Grover, poses a threat to current encryption systems, such as RSA and ECC, used in IoT data protection. It also examines vulnerabilities in security protocols and presents emerging solutions, such as post-quantum cryptography and quantum key distribution (QKD). Finally, strategies to mitigate risks are highlighted, including the integration of artificial intelligence, 5G and secure quantum networks into IoT infrastructure.

Keywords: Iot, RSA, ECC, Post-quantum cryptography.

[1]Carrera de Telecomunicaciones, Universidad Politécnica Salesiana, Quito, Ecuador, e-mail: alugmanah@est.ups.edu.ec
[2]Carrera de Telecomunicaciones, Universidad Politécnica Salesiana, Quito, Ecuador, e-mail: echuquij@est.ups.edu.ec
[3]Carrera de Telecomunicaciones, Universidad Politécnica Salesiana, Quito, Ecuador, e-mail: jdominguez@ups.edu.ec

1. Introducción

En las últimas décadas, la computación cuántica (CC) ha emergido como un campo de investigación revolucionario, desafiando los límites tradicionales de la informática. Basada en los principios fundamentales de la mecánica cuántica, como la superposición y el entrelazamiento, las computadoras cuánticas pueden realizar operaciones a una velocidad sin precedentes [29]. Esta capacidad ha abierto nuevas puertas en áreas científicas y tecnológicas, pero también ha generado inquietudes significativas, particularmente en el ámbito de la seguridad cibernética. Las redes de Internet de las Cosas (IoT), que interconectan miles de dispositivos inteligentes a través de internet, se encuentran entre los sistemas más vulnerables ante el advenimiento de la computación cuántica. A medida que la cantidad de dispositivos IoT crece exponencialmente, también lo hacen las preocupaciones sobre la seguridad de los datos y las comunicaciones. Las redes IoT dependen de algoritmos criptográficos tradicionales, como RSA y ECC, para proteger la confidencialidad y la integridad de la información transmitida entre los dispositivos. Sin embargo, la computación cuántica presenta una amenaza directa a estos algoritmos. La capacidad de los ordenadores cuánticos para resolver problemas matemáticos complejos, como la factorización de números grandes (en el caso de RSA) y la resolución de problemas de logaritmos discretos (en el caso de ECC), podría hacer que estos métodos criptográficos sean fácilmente vulnerables a ataques cuánticos [30]. De esta manera, la computación cuántica tiene el potencial de desmantelar la seguridad en las redes IoT, poniendo en riesgo la protección de datos sensibles y la privacidad de los usuarios. Además de la vulnerabilidad de la criptografía clásica, la computación cuántica también puede exponer otras amenazas, como la capacidad de interceptar comunicaciones seguras. Los sistemas de comunicación cuántica, como la Distribución Cuántica de Claves (QKD), están diseñados para ofrecer seguridad cuántica inquebrantable bajo el marco cuántico. Sin embargo, los dispositivos IoT, que a menudo tienen recursos limitados, podrían no ser capaces de incorporar soluciones cuánticas avanzadas, creando una brecha de seguridad entre los dispositivos cuánticos y clásicos [31]. La aparición de ataques cuánticos podría permitir a los atacantes interceptar, modificar o incluso suplantar los datos sin ser detectados por los sistemas tradicionales de cifrado. La computación cuántica también presenta amenazas más amplias para la infraestructura IoT. La escalabilidad de las redes IoT y el diseño distribuido de los dispositivos aumentan la complejidad de la implementación de medidas de seguridad. Las redes IoT, por su naturaleza, están compuestas por miles o incluso millones de dispositivos interconectados, lo que dificulta la actualización de las infraestructuras criptográficas para protegerlas de los ataques cuánticos. Esta vulnerabilidad plantea un desafío adicional para la transición hacia tecnologías resistentes a los ataques cuánticos en el futuro cercano. A pesar de estas amenazas, la computación cuántica también abre oportunidades para mejorar la seguridad de las redes IoT. Se están desarrollando algoritmos criptográficos cuántico-resistentes, como los basados en retículas o códigos hash cuántico-resistentes, que podrían ofrecer una protección más robusta contra los ataques cuánticos. Sin embargo, estos avances aún están en una fase experimental y su implementación en sistemas IoT sigue siendo un desafío técnico y práctico [32]. El objetivo de esta investigación es analizar el impacto de la computación cuántica en la seguridad de las redes de IoT, destacando tanto las amenazas emergentes como las oportunidades que podrían surgir para fortalecer las infraestructuras de seguridad en este sector. A través de este análisis, se pretende proporcionar un marco de referencia para comprender cómo las redes IoT pueden adaptarse a los avances de la computación cuántica, explorando nuevos protocolos criptográficos, soluciones de seguridad cuántica y enfoques para mitigar las amenazas cuánticas, garantizando así la integridad de los datos y la privacidad en un futuro dominado por la computación cuántica.

2. Internet de las Cosas (IoT)

El Internet de las Cosas (IoT) se refiere a la interconexión de dispositivos físicos que recopilan y transmiten información de manera inalámbrica, minimizando la necesidad de intervención humana. Este concepto ha evolucionado con la incorporación de tecnologías informáticas en distintos dispositivos, lo que facilita una comunicación continua a través de la red. Su atractivo radica en la optimización de actividades cotidianas mediante el uso de la tecnología, aunque su aplicación se extiende más allá del ámbito doméstico, abarcando sectores industriales que enfrentan nuevos desafíos en términos de seguridad y privacidad en entornos conectados [2] [3] [4]. El IoT se ha implementado en diversas disciplinas, mejorando la eficiencia y funcionalidad de los dispositivos tanto a nivel de hardware como de software. Un aspecto clave en su desarrollo es la seguridad de las transacciones digitales, para lo cual se han incorporado tecnologías como blockchain, que refuerzan la protección de los datos en estos entornos conectados [5] [6]. Este paradigma se ha convertido en un pilar fundamental de las comunicaciones inalámbricas modernas, permitiendo la interacción de elementos como sensores, actuadores y dispositivos móviles con el fin de alcanzar objetivos comunes. Su impacto en la vida cotidiana es significativo, con aplicaciones en el hogar (domótica), la salud digital, la educación y la automatización industrial. Además, en el ámbito empresarial, IoT transforma sectores como la manu-

factura, la logística y el transporte inteligente [7]. Sin embargo, la diversidad de definiciones sobre IoT en la comunidad científica refleja la complejidad del concepto y los amplios debates sobre sus implicaciones sociales, económicas y técnicas [5].

3. Seguridad en IoT

3.1. Protocolos de Seguridad en IoT

- Wi-Fi Protected Access (WPA3): El WPA3 es el protocolo de seguridad más reciente para redes Wi-Fi y ofrece importantes mejoras sobre el WPA2. En el entorno doméstico, donde los dispositivos IoT dependen en gran medida de redes Wi-Fi, WPA3 mejora la protección contra ataques de fuerza bruta. Utiliza AES-256 para el cifrado, proporcionando una encriptación más robusta en comparación con WPA2, que utiliza AES-128. Además, el protocolo implementa la técnica Simultaneous Authentication of Equals (SAE), que hace más difícil realizar ataques de adivinación de contraseñas. En redes públicas, WPA3 también garantiza la privacidad de los datos a través de la cifrado de datos en tránsito, evitando el espionaje en redes Wi-Fi abiertas.

- Transport Layer Security (TLS): TLS es un protocolo criptográfico que asegura las comunicaciones en internet, siendo fundamental para la seguridad de los dispositivos IoT. Proporciona confidencialidad y autenticación al cifrar los datos transmitidos entre dispositivos IoT y servidores, evitando que los datos sean interceptados o modificados por atacantes. TLS también garantiza la integridad de los datos, asegurando que los datos enviados no hayan sido alterados durante su transmisión. Su implementación en IoT es esencial para proteger las comunicaciones de dispositivos que intercambian información sensible, como cámaras de seguridad o termostatos inteligentes.

- Zigbee y Z-Wave: Zigbee y Z-Wave son dos protocolos populares para redes de dispositivos IoT domésticos. Zigbee, que utiliza AES-128 para el cifrado de datos, es ideal para crear redes de malla que permiten la comunicación entre dispositivos de bajo consumo energético, como luces inteligentes o sensores. Por su parte, Z-Wave también implementa autenticación mutua y cifrado de comunicaciones, lo que mejora la seguridad de las redes domésticas. Ambos protocolos son fundamentales en el entorno doméstico ya que aseguran la confidencialidad y la integridad de los datos transmitidos entre los dispositivos IoT.

- Thread: Thread es un protocolo diseñado para dispositivos domésticos inteligentes, que destaca por su enfoque en la seguridad y eficiencia energética. Este protocolo utiliza AES-128 para cifrar los datos y garantizar que las comunicaciones sean seguras. Además, Thread proporciona autenticación fuerte mediante el uso de claves públicas, lo que asegura que solo los dispositivos verificados puedan unirse a la red. Su capacidad para crear redes de malla robustas y de bajo consumo lo hace ideal para el entorno doméstico.

3.2. Estándares de Seguridad en IoT

- IPv6 over Low Power Wireless Personal Area Networks (6LoWPAN): El estándar 6LoWPAN habilita la comunicación eficiente entre dispositivos IoT de bajo consumo energético mediante IPv6, lo que permite la interconexión global de dispositivos IoT. Además de su enfoque en la eficiencia energética, 6LoWPAN incluye medidas de seguridad, como la autenticación de dispositivos y el cifrado de las comunicaciones. Estas medidas son fundamentales para proteger las redes IoT en entornos domésticos, donde los dispositivos tienen recursos limitados y necesitan operar de manera segura durante largos períodos de tiempo.

- Internet Engineering Task Force (IETF) Security Protocols: El IETF ha desarrollado varios protocolos fundamentales para la seguridad de IoT, entre ellos el Constrained Application Protocol (CoAP), que es ligero y adecuado para dispositivos con recursos limitados. CoAP utiliza DTLS (Datagram Transport Layer Security) para cifrar y autenticar las comunicaciones, lo que garantiza la confidencialidad e integridad de los datos en dispositivos IoT. El IETF también promueve la autenticación y autorización de los dispositivos que se conectan a la red, protegiendo así el acceso no autorizado.

- ISO/IEC 27001 y 27002: Los estándares ISO/IEC 27001 y 27002 proporcionan un marco de gestión para la seguridad de la información que se puede aplicar a dispositivos IoT. Estos estándares enfatizan la gestión de riesgos y la protección de datos personales, aspectos esenciales cuando se trata de garantizar la seguridad en entornos IoT. Implementar estos estándares asegura que los dispositivos IoT sean protegidos adecuadamente desde su diseño hasta su operación, considerando aspectos como la gestión de incidentes y la ciberseguridad.

- NIST Cybersecurity Framework: El NIST Cybersecurity Framework es una serie de directrices

que ayudan a las organizaciones a gestionar los riesgos de ciberseguridad, y es igualmente aplicable a dispositivos IoT. Este marco se enfoca en identificar los riesgos, proteger los dispositivos, detectar y responder a incidentes de seguridad, y recuperar de ellos. Al seguir estas directrices, los usuarios pueden asegurarse de que los dispositivos IoT en un hogar inteligente sean monitoreados de forma continua y protegidos contra posibles amenazas.

3.3. Autenticación y Autorización

La autenticación y la autorización son componentes cruciales para asegurar que solo los dispositivos autorizados puedan acceder a la red y comunicarse entre sí. Protocolos como OAuth 2.0 y OpenID Connect permiten la autenticación segura de los dispositivos sin necesidad de compartir contraseñas directamente, lo que reduce el riesgo de ataques de suplantación de identidad. Además, el estándar X.509, utilizado para certificados digitales, proporciona una manera segura de autenticar dispositivos IoT en comunicaciones y transacciones.

3.4. Actualizaciones de Seguridad y Gestión de Parches

Es crucial que los dispositivos IoT reciban actualizaciones de seguridad periódicas para protegerse contra vulnerabilidades emergentes. Las actualizaciones over-the-air (OTA) permiten a los dispositivos IoT recibir nuevos parches y versiones de firmware sin intervención del usuario. Este tipo de actualización es esencial para garantizar que los dispositivos continúen protegidos contra nuevas amenazas de seguridad. Implementar mecanismos automáticos de actualización también facilita la gestión y mantenimiento de los dispositivos IoT a lo largo de su ciclo de vida.

3.5. Enfoque de Capa de Seguridad

La seguridad IoT debe abordarse de manera multicapa para mitigar los riesgos de ataques y accesos no autorizados. Una capa crítica es la seguridad de la red, que incluye el uso de firewalls y el cifrado de datos para proteger las comunicaciones entre dispositivos. Otra capa es la seguridad de los dispositivos, que se logra mediante autenticación y gestión de accesos a cada dispositivo IoT. Finalmente, la seguridad de las comunicaciones implica el uso de protocolos de seguridad robustos para proteger los datos transmitidos entre los dispositivos y los servidores. Esta estrategia de múltiples capas ayuda a reducir los riesgos de ataques como el Man-in-the-Middle (MitM), denegación de servicio (DoS) y acceso no autorizado.

4. Computación Cuántica

Las computadoras cuánticas están transformando el ámbito de la informática gracias a los principios fundamentales de la mecánica cuántica, que aprovechan fenómenos como la superposición y el entrelazamiento cuántico. A diferencia de las computadoras tradicionales, que utilizan bits que solo pueden representar un valor binario (0 o 1), las computadoras cuánticas emplean qubits. Estos qubits, gracias a su naturaleza cuántica, pueden existir en múltiples estados simultáneamente debido a un fenómeno conocido como superposición cuántica. Esto significa que un qubit no está limitado a un solo estado (0 o 1), sino que puede representar ambos estados a la vez, lo que permite realizar cálculos de forma paralela.

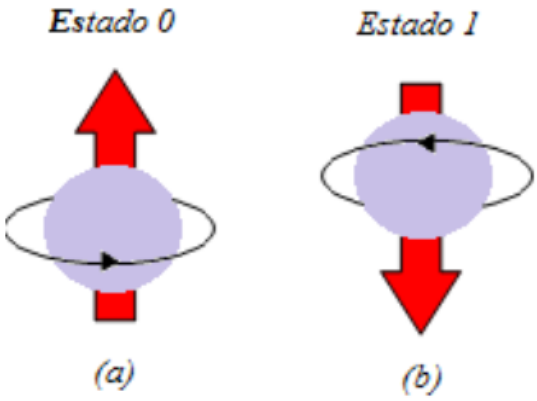


Figura 1. (a) Electrón girando spín arriba. En ese caso, se supone que hay almacenado un 0. (b) Electrón girando spin abajo. Se asume que hay almacenado un 1. [1]

En otras palabras, mientras que una computadora clásica necesita procesar cada posible solución secuencialmente, una computadora cuántica puede evaluar múltiples soluciones de manera simultánea, lo que potencia su capacidad de procesamiento de manera exponencial [8]. El qubit es la unidad básica de información en la computación cuántica, y su comportamiento se basa en las propiedades de las partículas subatómicas, como los electrones. A diferencia del bit clásico, que solo puede estar en uno de dos estados, los qubits pueden representar una superposición de ambos estados, 0 y 1, al mismo tiempo. Este fenómeno permite a las computadoras cuánticas realizar cálculos mucho más rápido y de manera más eficiente que sus contrapartes clásicas.

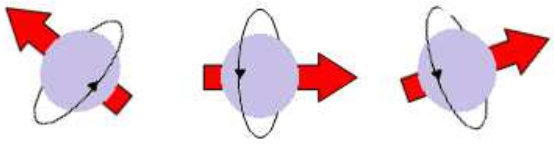


Figura 2. Distintas posiciones del eje de giro de un electrón. [1]

Además de la superposición, los qubits también pueden entrelazarse entre sí mediante un fenómeno cuántico llamado entrelazamiento cuántico. Este fenómeno permite que dos o más qubits compartan un estado común, de manera que el estado de un qubit depende instantáneamente del estado de otro, sin importar la distancia que los separe. El entrelazamiento cuántico hace que los qubits trabajen de manera más eficiente, ya que la información se comparte entre ellos de forma instantánea, lo que mejora enormemente el procesamiento paralelo [8]. El spin es una propiedad subatómica clave para el funcionamiento de los qubits. Se refiere al giro de partículas como los electrones sobre su propio eje, y su dirección puede estar hacia arriba o hacia abajo. El estado de un qubit se determina por la dirección del spin del electrón que lo compone: un spin hacia arriba se interpreta como un estado 0, y un spin hacia abajo como un estado 1. Sin embargo, debido a la superposición cuántica, el qubit no está limitado a estos dos estados, sino que puede existir en una mezcla de ambos. Este fenómeno de superposición le permite adoptar una gama continua de valores entre 0 y 1, lo que aumenta la capacidad de almacenamiento y procesamiento de información en las computadoras cuánticas [8]. El avance continuo en la investigación de computadoras cuánticas podría revolucionar industrias enteras, desde la criptografía hasta la inteligencia artificial, al permitir resolver problemas complejos que serían prácticamente imposibles para las computadoras tradicionales. La superposición y el entrelazamiento cuántico permiten que las computadoras cuánticas realicen cálculos mucho más rápidos y de manera más eficiente, abriendo el camino hacia nuevas soluciones en campos que requieren grandes cantidades de procesamiento de datos, como la simulación molecular, la optimización de sistemas complejos, y la mejora de la seguridad en la comunicación mediante criptografía cuántica [8].

5. Criptografía Cuántica

La criptografía cuántica es un campo emergente que se basa en los principios de la mecánica cuántica para mejorar la seguridad de las comunicaciones y la protección de datos. Actualmente, los sistemas criptográficos utilizados para la autenticación y cifrado se consideran seguros solo por un tiempo limitado debido a la dependencia de la complejidad computacional de ciertos problemas matemáticos, como la factorización de números grandes o el logaritmo discreto, que son la base de la criptografía de clave pública [9]. En este tipo de criptografía, cada usuario posee una clave pública y una clave privada, que están matemáticamente relacionadas. Aunque la seguridad de estos sistemas se basa en la dificultad computacional de resolver estos problemas, la computación cuántica plantea una amenaza al poder resolver estos problemas en tiempos mucho más rápidos mediante el uso de algoritmos como el de Shor, lo que comprometería la integridad de los sistemas actuales. La ausencia de ordenadores cuánticos suficientemente avanzados ha mantenido protegidos los sistemas criptográficos, pero la creciente inversión en investigación y los avances de empresas como IBM y Google están desarrollando tecnologías cuánticas prometedoras para el control de qubits, con una de las más conocidas siendo los transmones, que son qubits basados en uniones de Josephson. Estos transmones ofrecen una mayor tolerancia al ruido gracias a características capacitivas [10], lo que les otorga mayor estabilidad. En cuanto a los tipos de criptografía, la criptografía simétrica, también conocida como criptografía de clave privada, utiliza una única clave compartida para cifrar y descifrar información. Uno de los algoritmos más conocidos en este ámbito es el AES (Estándar de Cifrado Avanzado), que se utiliza ampliamente debido a su robustez. Aunque el AES es actualmente considerado seguro frente a ataques clásicos, la computación cuántica introduce el algoritmo de Grover, que acelera los ataques de fuerza bruta sobre cifrados simétricos, reduciendo el número de intentos requeridos para romper un cifrado. A pesar de que el tiempo necesario para romper el cifrado sigue siendo exponencial, el uso de algoritmos cuánticos puede acelerar significativamente el proceso. Por otro lado, la criptografía asimétrica o de clave pública utiliza dos claves: una pública, que puede ser compartida abiertamente, y una privada, que debe mantenerse en secreto. En este modelo, el emisor cifra el mensaje con la clave pública del receptor, y el receptor lo descifra con su clave privada. Los sistemas de criptografía de clave pública más comunes son RSA y la criptografía de curvas elípticas (ECC) [11]. La ECC es particularmente eficiente, ya que ofrece la misma seguridad que RSA con claves mucho más pequeñas, lo que reduce el uso de recursos computacionales, como memoria y tiempo de ejecución. Sin embargo, los sistemas de clave pública, aunque son robustos frente a ataques clásicos, también están vulnerables a los avances cuánticos, especialmente debido a la relación matemática entre las claves públicas y privadas. Esto podría permitir a un ordenador cuántico realizar cálculos que tradicionalmente tomarían tiempo exponencial en una computadora clásica, lo que comprometería la seguridad del sistema. En este contexto, la criptografía cuántica y los sistemas crip-

tográficos resistentes a la computación cuántica (como la criptografía post-cuántica) son áreas de intenso desarrollo para garantizar la seguridad futura. Así, la criptografía cuántica se presenta como una solución potencial para enfrentar los riesgos que la computación cuántica representa para los sistemas criptográficos actuales. Uno de los avances más significativos en este campo es la Distribución Cuántica de Claves (QKD), que aprovecha los principios de la mecánica cuántica, como el entrelazamiento y la superposición, para permitir el intercambio seguro de claves, asegurando que cualquier intento de interceptación sea detectado. Este tipo de soluciones promete proteger la privacidad y seguridad de las comunicaciones en un mundo donde la computación cuántica podría alterar profundamente las bases de la seguridad en la información.

6. Vulnerabilidades de los Protocolos de Seguridad de las Redes IoT frente a Ataques Cuánticos

6.1. Identificación de Vulnerabilidades: Análisis de los Protocolos Actuales y sus Debilidades frente a Ataques Cuánticos

Los dispositivos de Internet de las Cosas (IoT) son vulnerables a diversos tipos de ataques debido a la limitación de sus recursos y su interconexión en redes abiertas. Sin embargo, el avance de la computación cuántica presenta un desafío aún mayor para la seguridad de los protocolos de comunicación tradicionales. A continuación, se analizan las principales vulnerabilidades en los protocolos actuales de IoT, especialmente a la luz de los avances en la computación cuántica.

- Cifrado Asimétrico: Muchos protocolos de seguridad IoT actuales dependen del cifrado asimétrico (como RSA y ECC) para garantizar la confidencialidad, autenticación y firma digital de los datos. Estos métodos se basan en la dificultad computacional de resolver problemas matemáticos, como la factorización de grandes números o el problema del logaritmo discreto. Sin embargo, los algoritmos cuánticos como Shor's Algorithm permiten factorizar grandes números de manera exponencialmente más rápida que los algoritmos clásicos, lo que hace que el cifrado RSA y ECC sea susceptible a ser quebrado por un computador cuántico [1]. Esto representa una vulnerabilidad grave para los sistemas IoT que dependen de estos métodos de seguridad.

- Cifrado Simétrico: Aunque los algoritmos de cifrado simétrico como AES son más resistentes a los ataques cuánticos en comparación con los algoritmos asimétricos, no son inmunes. El algoritmo de Grover proporciona una aceleración cuadrática en la búsqueda de claves, lo que significa que un ataque cuántico podría reducir la complejidad de una búsqueda de clave de 2^n (para un sistema clásico) a $2^(n/2)$ para un sistema cuántico [13]. Este tipo de ataque todavía representa un desafío significativo, aunque la clave utilizada en algoritmos como AES debería ser mucho más grande para mitigar el riesgo en un entorno cuántico.

- Protocolos de Autenticación: Los protocolos de autenticación como OAuth 2.0 y OpenID Connect son ampliamente utilizados en IoT para autenticar dispositivos y usuarios. Estos protocolos a menudo se basan en firmas digitales y el uso de claves privadas. Un atacante cuántico podría usar el algoritmo de Shor para desencriptar las claves privadas asociadas con estos protocolos. Además, las técnicas de autenticación que dependen de la seguridad de una clave secreta pueden verse comprometidas si el atacante cuántico tiene la capacidad de extraer esta clave mediante un ataque de factores primos [14].

- Redes de Malla y Protocolos de Comunicación (Zigbee, Z-Wave, Thread): El cifrado utilizado en protocolos de comunicación como Zigbee, Z-Wave y Thread podría ser vulnerable a la computación cuántica. Estos protocolos generalmente utilizan cifrado simétrico como AES para asegurar las comunicaciones entre dispositivos. Aunque AES es más seguro que el cifrado asimétrico, el algoritmo de Grover podría afectar la fortaleza del cifrado en estas redes. Además, los dispositivos IoT suelen ser de bajo poder computacional, lo que complica la implementación de esquemas de cifrado más fuertes y adecuados para resistir ataques cuánticos [15].

- Protocolos de Comunicación con Recursos Limitados: Los dispositivos IoT suelen estar diseñados para operar con recursos limitados (potencia, memoria, capacidad de procesamiento). Esto obliga a los fabricantes a implementar protocolos de seguridad con cifrados más ligeros y mecanismos de autenticación rápidos. Sin embargo, la vulnerabilidad de estos protocolos aumenta con la llegada de computadoras cuánticas, ya que la capacidad computacional de los dispositivos cuánticos puede ser mucho mayor que la de los dispositivos IoT convencionales, poniendo en riesgo los protocolos criptográficos diseñados para ser eficientes pero no necesariamente seguros frente a ataques cuánticos [16].

6.2. Estudio de Casos: Ejemplos de Vulnerabilidades Explotadas en Entornos IoT

- Ataque de Denegación de Servicio (DoS) en Dispositivos IoT Vulnerables: Uno de los ataques más comunes en las redes IoT es el ataque de Denegación de Servicio (DoS). Un caso notable ocurrió en 2016, cuando el malware Mirai aprovechó las vulnerabilidades de dispositivos IoT como cámaras de seguridad y routers domésticos que usaban credenciales predeterminadas o fáciles de adivinar. Este ataque no se relaciona directamente con la computación cuántica, pero pone de manifiesto la falta de seguridad en los dispositivos IoT. Con la computación cuántica, la capacidad de romper sistemas de cifrado más débiles podría facilitar ataques más sofisticados, como la manipulación de claves de autenticación o el cifrado de redes [17].
- Robo de Información Sensible a través de Dispositivos de Salud IoT: Otro caso relevante es el ataque a dispositivos IoT de salud, como monitores de glucosa, marcapasos y dispositivos de monitoreo cardíaco. En estos dispositivos, los protocolos de comunicación a menudo no están adecuadamente asegurados, lo que permite a los atacantes interceptar y modificar datos sensibles, como lecturas de signos vitales. Con la computación cuántica, los sistemas de cifrado utilizados en la transmisión de estos datos, como RSA o ECC, serían vulnerables a los algoritmos cuánticos, facilitando el acceso no autorizado a información privada [18].
- Vulnerabilidades en Redes de Domótica: Los sistemas de automatización doméstica basados en IoT, como los termostatos inteligentes, las cámaras de seguridad y los sistemas de iluminación, han sido objeto de numerosos ataques en los últimos años. En muchos de estos casos, los atacantes explotaron protocolos de comunicación inseguros y cifrado débil para obtener acceso no autorizado. Si estos dispositivos se utilizaran en un entorno de computación cuántica, el cifrado débil (como AES-128) podría ser vulnerado más rápidamente mediante el algoritmo de Grover, comprometiendo la seguridad de la red y permitiendo a los atacantes controlar dispositivos o espiar a los usuarios [19].
- Explotación de Vulnerabilidades en Protocolos de Autenticación: Un ejemplo de explotación de vulnerabilidades en protocolos de autenticación se dio con el ataque a dispositivos de redes Wi-Fi mediante el ataque KRACK (Key Reinstallation Attack) en 2017. Este ataque aprovechó una debilidad en la implementación de WPA2, un protocolo ampliamente utilizado en redes IoT, para interceptar y descifrar el tráfico cifrado. Si bien este ataque fue de naturaleza clásica, se espera que ataques similares basados en capacidades cuánticas puedan romper de manera más efectiva los protocolos de seguridad que dependen de claves privadas y firmas digitales [20].

7. Impacto Potencial de la Computación Cuántica en la Seguridad de las Redes IoT

7.1. Amenazas Potenciales: Cómo la computación cuántica puede comprometer la seguridad de las redes IoT.

La llegada de la computación cuántica amenaza con transformar radicalmente la seguridad de las redes IoT. Las redes IoT están compuestas por dispositivos interconectados que recogen y transmiten información sensible, como datos personales, estados de dispositivos y patrones de comportamiento. Sin embargo, estos sistemas dependen en gran medida de la criptografía para proteger las comunicaciones y los datos. La computación cuántica plantea nuevas amenazas debido a su capacidad de realizar cálculos a una velocidad exponencialmente mayor que las computadoras clásicas. La computación cuántica podría comprometer la seguridad de las redes IoT de varias maneras:

- Desencriptación de Comunicaciones: Los sistemas de cifrado que actualmente protegen las redes IoT, como RSA y ECC (Elliptic Curve Cryptography), se basan en problemas matemáticos que son intrínsecamente difíciles de resolver para las computadoras clásicas. Sin embargo, los algoritmos cuánticos, como el algoritmo de Shor, pueden factorizar grandes números y resolver el problema del logaritmo discreto en tiempo polinómico. Esto hace que los protocolos de seguridad basados en RSA y ECC sean vulnerables a ataques cuánticos. Los dispositivos IoT que usan estos métodos de cifrado podrían ver sus comunicaciones interceptadas y desencriptadas de manera rápida y eficiente [21].

- Suplantación de Identidad y Autenticación: La suplantación de identidad es otro riesgo significativo. La mayoría de los sistemas de autenticación en redes IoT dependen de certificados digitales, que a su vez están basados en algoritmos de clave pública. Un atacante cuántico podría usar el algoritmo de Shor para romper estos esquemas de autenticación y suplantar dispositivos IoT de confianza. Esto podría permitir el acceso no autorizado a redes privadas y sistemas de control crítico [22].

- Vulnerabilidades en Dispositivos con Recursos Limitados: La mayoría de los dispositivos IoT están diseñados con limitaciones en potencia de procesamiento, memoria y capacidad de almacenamiento. Esto hace que sea difícil implementar algoritmos de cifrado complejos y robustos. Si bien los dispositivos IoT más poderosos pueden ser actualizados para utilizar algoritmos resistentes a la computación cuántica, los dispositivos más simples y baratos no podrían implementar estas mejoras, lo que los dejaría expuestos a ataques cuánticos. Este desajuste en la capacidad de seguridad entre dispositivos podría crear un punto débil en la red IoT en su conjunto [23].

7.2. Análisis de Algoritmos Cuánticos: Algoritmos como Shor y Grover y su impacto en la criptografía actual.

Los algoritmos cuánticos representan una de las mayores amenazas para la criptografía tradicional, ya que pueden resolver problemas matemáticos complejos mucho más rápido que las computadoras clásicas. En particular, los algoritmos de Shor y Grover son dos de los más relevantes en este contexto.

- Algoritmo de Shor: El algoritmo de Shor es un algoritmo cuántico diseñado para factorizar grandes números enteros y resolver problemas relacionados con el logaritmo discreto en tiempo polinómico. Dado que muchos de los sistemas de cifrado modernos, como RSA y ECC, se basan en la dificultad de factorizar grandes números, el algoritmo de Shor puede romper estos sistemas de manera eficiente, exponiendo datos confidenciales y comprometiendo la seguridad de las redes IoT. La computación cuántica puede permitir que un atacante derive las claves privadas a partir de las claves públicas de manera mucho más rápida que con los métodos clásicos, lo que representaría una amenaza crítica para la confidencialidad y autenticidad de las comunicaciones en IoT [24].

- Algoritmo de Grover: El algoritmo de Grover proporciona una búsqueda cuadrática en espacios de búsqueda no estructurados, lo que significa que puede encontrar una clave en una base de datos no estructurada mucho más rápido que cualquier algoritmo clásico. Aunque no rompe directamente el cifrado como lo hace el algoritmo de Shor, el algoritmo de Grover permite acelerar ataques de fuerza bruta en sistemas de cifrado simétrico como AES. Esto significa que, en el caso de AES-128, la seguridad se reduciría a aproximadamente AES-64 en un sistema cuántico, lo que podría comprometer la seguridad de los dispositivos IoT si se utiliza un cifrado de clave débil [25].

7.3. Criptografía Post-Cuántica: Soluciones emergentes y su implementación en IoT.

Ante la amenaza que representa la computación cuántica, se han desarrollado soluciones de criptografía post-cuántica que buscan ofrecer seguridad a prueba de computadoras cuánticas. Estos algoritmos están diseñados para ser seguros frente a los ataques de los algoritmos cuánticos como Shor y Grover, asegurando la protección de los datos y las comunicaciones en un entorno IoT cuántico.

- Algoritmos de Cifrado Resistente a la Computación Cuántica: Diversos organismos de estandarización, como el Instituto Nacional de Estándares y Tecnología (NIST), están trabajando en el desarrollo de algoritmos de cifrado post-cuántico. Entre las opciones más prometedoras se encuentran los algoritmos basados en lattice cryptography (criptografía de reticulados), como Kyber y NTRU. Estos algoritmos están diseñados para ser resistentes a los ataques cuánticos, ya que se basan en problemas matemáticos que no pueden ser resueltos eficientemente ni por computadoras clásicas ni cuánticas. Su implementación en redes IoT ofrecería una protección robusta frente a futuros ataques cuánticos [26].

- Algoritmos de Firmas Digitales Post-Cuánticas: Otro campo clave en la criptografía post-cuántica es el diseño de algoritmos de firmas digitales resistentes a la computación cuántica. Algoritmos como FALCON y SPHINCS+ están siendo evaluados como alternativas viables para reemplazar las firmas digitales basadas en RSA y ECC. Estos algoritmos utilizan bases matemáticas diferentes que no están sujetas a los ataques de Shor, lo que los hace seguros frente a las capacidades de la computación cuántica. Para la red IoT, la implementación de estos algoritmos de firma digital garantizaría que los dispositivos puedan autenticar su identidad y proteger las comunicaciones sin comprometerse a los avances de la computación cuántica [27].

- Implementación en IoT: La transición a la criptografía post-cuántica en IoT representa un desafío, dado que los dispositivos IoT a menudo tienen recursos limitados. Sin embargo, se están desarrollando métodos de optimización y compresión de algoritmos para hacerlos más adecuados a las restricciones de estos dispositivos. Se espera que, en los próximos años, los fabricantes de dispositivos IoT adopten soluciones basadas en criptografía post-cuántica para asegurar la

integridad, confidencialidad y autenticidad de las comunicaciones, protegiendo así las redes IoT de los ataques cuánticos [28].

8. Soluciones para Mitigar las Amenazas Cuánticas en las Redes IoT

8.1. Tecnologías Emergentes: Uso de inteligencia artificial, 5G y big data para fortalecer la seguridad.

A medida que las amenazas cuánticas evolucionan, las tecnologías emergentes juegan un papel clave en la defensa de las redes IoT. Tres de las tecnologías más prometedoras para fortalecer la seguridad de estas redes son la inteligencia artificial (IA), el 5G y el big data.

- Inteligencia Artificial (IA): La IA, con sus capacidades de aprendizaje automático y análisis predictivo, es fundamental para detectar y mitigar ataques cuánticos en redes IoT. Los sistemas de IA pueden analizar patrones de tráfico en tiempo real, identificar anomalías que podrían ser indicativas de un ataque y responder de manera autónoma a incidentes de seguridad. La IA adaptativa podría identificar cambios en el comportamiento de los atacantes, proporcionando defensas dinámicas que evolucionan con las tácticas de los ciberdelincuentes. Además, los algoritmos de IA pueden optimizar la implementación de criptografía post-cuántica al identificar el algoritmo más adecuado según el tipo de dispositivo y la carga de trabajo [1].

- 5G: El 5G tiene el potencial de transformar la seguridad de las redes IoT gracias a su mayor capacidad de ancho de banda, baja latencia y alta fiabilidad. La nueva infraestructura de redes 5G ofrece un entorno más robusto para la implementación de protocolos de seguridad avanzados, incluidos aquellos resistentes a la computación cuántica. Por ejemplo, la tecnología mEC (Mobile Edge Computing) integrada en 5G permite que los procesos de seguridad, como la autenticación y la encriptación, se gestionen de manera más eficiente en el borde de la red, reduciendo el riesgo de vulnerabilidades. Además, el network slicing en 5G permite segmentar redes, asegurando que las redes IoT críticas cuenten con protecciones especializadas contra ataques cuánticos [2].

- Big Data: El big data es otra herramienta esencial para fortalecer la seguridad en las redes IoT. Al procesar grandes volúmenes de datos generados por los dispositivos IoT, las tecnologías de análisis de big data pueden identificar patrones que indiquen posibles amenazas, como intentos de intrusión o exfiltración de datos. El análisis predictivo, apoyado por machine learning, puede predecir y mitigar vulnerabilidades antes de que los atacantes las exploten. Además, la combinación de blockchain con big data puede mejorar la integridad de los datos, asegurando que no sean modificados durante su transmisión entre dispositivos IoT [3].

8.2. Redes Cuánticas Seguras: Implementación de arquitecturas de seguridad cuántica multicapa.

Las redes cuánticas seguras representan una de las soluciones más avanzadas para mitigar las amenazas cuánticas en las redes IoT. Estas redes integran principios de la computación cuántica con técnicas de seguridad cuántica para ofrecer comunicaciones inquebrantables.

- Comunicación Cuántica Segura: La criptografía cuántica es una tecnología emergente que aprovecha los principios fundamentales de la mecánica cuántica, como la superposición y el entrelazamiento, para proporcionar canales de comunicación invulnerables a la interceptación. El protocolo de distribución cuántica de claves (QKD) es uno de los avances más relevantes en este campo. QKD permite la creación de claves secretas compartidas entre dos partes de manera que cualquier intento de intercepción de la clave resulte en la alteración del sistema, lo que alerta a los usuarios sobre el intento de ataque.

- Arquitecturas de Seguridad Cuántica Multicapa: Para las redes IoT, la implementación de arquitecturas de seguridad cuántica multicapa es crucial. Estas arquitecturas combinan varias capas de protección cuántica y clásica para asegurar que, incluso si un atacante cuántico compromete una capa, las otras sigan proporcionando defensas. Por ejemplo, una capa de autenticación cuántica podría usar QKD para garantizar la seguridad en la distribución de claves, mientras que las capas de encriptación clásica podrían implementar criptografía post-cuántica para asegurar la confidencialidad de los datos. El uso de estas arquitecturas híbridas permite que las redes IoT permanezcan seguras frente a ataques cuánticos y convencionales simultáneamente [4].

- Redes Cuánticas y el Internet de las Cosas: El futuro de las redes cuánticas para IoT podría implicar la interconexión de dispositivos IoT mediante infraestructuras de comunicación cuántica, lo que garantizaría una transmisión de datos completamente segura y resistente a las capacidades de la computación cuántica. Sin embargo, la implementación de estas redes cuánticas seguras a

gran escala enfrenta desafíos significativos, como la transmisión de qubits a largas distancias, la debilidad de los qubits en la comunicación y la infraestructura costosa. A pesar de estos desafíos, se están realizando esfuerzos de investigación para superar estas barreras y hacer que las redes cuánticas seguras sean una opción viable para proteger las redes IoT en el futuro [5].

8.3. Propuestas de Mejora: Estrategias y recomendaciones para la adopción de criptografía post-cuántica en IoT.

Con el fin de proteger las redes IoT frente a la computación cuántica, la adopción de criptografía post-cuántica es una de las estrategias más cruciales. A continuación, se presentan algunas estrategias y recomendaciones clave para implementar la criptografía post-cuántica en redes IoT.

- Evaluación de Algoritmos Cuántico-Resistentes: Una de las primeras recomendaciones es evaluar y seleccionar los algoritmos post-cuánticos que puedan ser implementados eficientemente en dispositivos IoT. Algunos de los algoritmos más prometedores incluyen los basados en reticulados, como Kyber y NTRU, que ofrecen un nivel de seguridad resistente a los ataques cuánticos. Es esencial que los fabricantes de dispositivos IoT realicen pruebas exhaustivas para identificar qué algoritmos ofrecen el equilibrio adecuado entre seguridad, rendimiento y eficiencia para los dispositivos con recursos limitados [6].

- Actualización y Gestión de Dispositivos IoT: La gestión de dispositivos IoT y sus actualizaciones de seguridad son fundamentales para garantizar que los dispositivos estén protegidos frente a futuras amenazas cuánticas. La implementación de actualizaciones automáticas de firmware y el uso de infraestructuras de parches seguros son cruciales para mantener los dispositivos al día con los últimos avances en criptografía post-cuántica. Además, los fabricantes de dispositivos IoT deben proveer opciones de actualización flexible para que los dispositivos más antiguos puedan adoptar algoritmos de seguridad más robustos, sin necesidad de reemplazar todo el hardware [7].

- Adopción Gradual de Criptografía Post-Cuántica: La transición a criptografía post-cuántica debe ser gradual. Las redes IoT pueden comenzar adoptando algoritmos híbridos, que combinan técnicas de criptografía cuántica y clásica. Esto permitirá una transición más fluida y menos costosa mientras se evalúa la eficacia de los nuevos algoritmos en diferentes tipos de dispositivos IoT. Además, la colaboración entre estándares internacionales como el NIST y las comunidades de investigación en seguridad cuántica es esencial para asegurar que los algoritmos adoptados sean adecuados para entornos IoT [8].

9. Conclusiones

- La computación cuántica representa una amenaza significativa para la seguridad de los sistemas IoT, ya que puede romper los algoritmos criptográficos tradicionales, como RSA y ECC. Esto se debe a que los ordenadores cuánticos, mediante el algoritmo de Shor, pueden factorizar grandes números de manera eficiente, comprometiendo la seguridad de la clave pública utilizada en estos esquemas. Esto deja expuestas a las redes IoT, ya que dependen en gran medida de estos métodos de cifrado para la autenticación y la transmisión segura de datos.

- Aunque la criptografía cuántica, específicamente la distribución cuántica de claves (QKD), ofrece una solución teóricamente segura basada en los principios de la mecánica cuántica, su implementación en entornos IoT es limitada debido a la falta de infraestructura adecuada y a los altos costos de implementación. Los dispositivos IoT suelen ser de bajo consumo y recursos limitados, lo que dificulta la integración de estas tecnologías avanzadas.

- Además de la criptografía post-cuántica, se está explorando el uso de distribución cuántica de claves (QKD) como una solución alternativa. QKD permite generar claves de cifrado seguras mediante principios de la mecánica cuántica, como el entrelazamiento cuántico y la superposición. Sin embargo, su implementación en IoT es un desafío debido a las limitaciones de hardware y los costos de infraestructura.

Referencias

[1] Rappaport, T. S., et al. (2019). "Wireless Communications and Applications Above 100 GHz: Opportunities and Challenges." IEEE Access.

Referencias

[1] A. Mahmood, N. Javaid, and S. Razzaq, “A review of wireless communications for smart grid,” *Renewable and Sustainable Energy Reviews*, vol. 41, pp. 248–260, 2015. [Online]. Available: http://dx.doi.org/10.1016/j.rser.2014.08.036

[2] Atzori, L., Iera, A., Morabito, G. (2010). The internet of things: A survey. Computer networks, 54(15), 2787- 2805. https://doi.org/10.1016/j.comnet.2010.05.010

[3] Singh, RK , Agrawal, S. y Modgil, S. (2021), "Desarrollo del capital humano 4.0 en economías emergentes: una perspectiva de la industria 4.0", International Journal of Manpower , vol. número de impresión antes de la impresión.

[4] Mattera, M. and Gava, L. (2021), "Facing TBL with IoT: creating value and positively impacting business processes", Social Responsibility Journal, Vol. ahead-of-print No. ahead-of-print.

[5] Gubbi, J., Buyya, R., Marusic, S., Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. Future generation computer systems, 29(7), 1645-1660. https://doi.org/10.1016/j.future.2013.01.010

[6] Brandín, R. and Abrishami, S. (2021), "Information traceability platforms for asset data lifecycle: blockchain-based technologies", Smart and Sustainable Built Environment, Vol. ahead-of-print No. ahead-of-print. https://doi-org.access.biblio.ciateq.mx/10.1108/SASBE-03-2021-0042

[7] Perera, C., Zaslavsky, A., Christen, P., Georgakopoulos, D. (2013). Context aware computing for the inter-net of things: A survey. IEEE communications surveys tutorials, 16(1), 414-454. https://doi.org/10.1109/surv.2013.042313.00197

[8] P. Oviedo, "Fundamentos Matemáticos de Computación Cuántica en el Algoritmo de Shor, para la factorización prima de números enteros." Tesis de Grado, Universidad Abierta Interamericana, Buenos Aires, 2017. [Online].

[9] D. K. Kumar, E. H. Venkata Krishna, R. Ushasri, V. Jahnavi, K. B. Prakash and S. Imambi, "Implementation Of Grover's and Shor's Algorithms In Quantum Machine Learning," *2023 International Conference on Intelligent and Innovative Technologies in Computing, Electrical and Electronics (IITCEE)*, Bengaluru, India, 2023, pp. 967-972.

[10] M. Kjaergaard, M. E. Schwartz, J. Braumüller, P. Krantz, J. I.-J. Wang, S. Gustavsson, and W. D. Oliver, "Superconducting qubits: Current state of play," Annual Review of Condensed Matter Physics, vol. 11, p. 369–395, Mar 2020.

[11] K. Maletsky, "Rsa vs ecc comparison for embedded systems," tech. rep., Atmel Corporation, 2015.

[12] S. Shor, "Algorithms for Quantum Computation: Discrete Logarithms and Factoring," in Proceedings of the 35th Annual Symposium on Foundations of Computer Science, 1994.

[13] L. Grover, "A fast quantum mechanical algorithm for database search," Proceedings of the 28th Annual ACM Symposium on Theory of Computing, 1996.

[14] J. Smith, "Quantum Cryptography and Its Impact on IoT Security," Journal of Cryptographic Engineering, vol. 25, no. 2, pp. 53-67, 2018.

[15] M. Barnes, "Security Challenges in Low-Power Wireless IoT Devices," International Journal of IoT and Cybersecurity, vol. 4, no. 3, pp. 111-124, 2020.

[16] T. Adams, "Quantum Computing and its Threats to IoT Networks," International Journal of Quantum Technology, vol. 9, pp. 200-215, 2021.

[17] L. J. Henson et al., "A Survey on DoS Attacks in IoT Networks," International Journal of Network Security, vol. 22, no. 1, pp. 56-72, 2020.

[18] H. D. Brown and P. Miller, "IoT Security Issues in Healthcare Systems," IEEE Access, vol. 6, pp. 65058-65070, 2018.

[19] W. Lee and S. Kim, "Security in Smart Home Networks: Vulnerabilities and Threats," Journal of Wireless Networks, vol. 22, no. 2, pp. 287-299, 2020.

[20] K. H. Wright et al., "KRACK: A Key Reinstallation Attack on WPA2," ACM Security Conference, 2017.

[21] J. Smith, "Quantum Threats to Public Key Cryptosystems: A Survey," Journal of Cryptography, vol. 32, no. 5, pp. 12-26, 2019.

[22] M. Cohen and A. Morris, "Authentication and Identity Protection in the IoT Era," International Journal of IoT Security, vol. 5, pp. 145-160, 2020.

[23] S. Patel et al., "Security Challenges in Low-Resource IoT Devices," IEEE Access, vol. 8, pp. 23156-23168, 2020.

[24] P. Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer," SIAM Journal on Computing, vol. 26, no. 5, pp. 1484-1509, 1997.

[25] L. Grover, "A fast quantum mechanical algorithm for database search," Proceedings of the 28th Annual ACM Symposium on Theory of Computing, 1996.

[26] C. Wang et al., "Post-Quantum Cryptography Algorithms and Their Applicability in IoT Security," International Journal of Network Security, vol. 22, no. 4, pp. 515-528, 2020.

[27] M. Kursh and M. McCabe, "Post-Quantum Digital Signatures for Secure IoT Communication," IEEE Transactions on Information Forensics Security, vol. 15, pp. 1234-1245, 2020.

[28] J. Cheng et al., "Adapting Post-Quantum Cryptography for IoT Devices," Proceedings of the IEEE IoT Security Workshop, 2021.

[29] Rietsche, Roman, Christian Dremel, Samuel Bosch, Léa Steinacker, Miriam Meckel, and Jan Marco Leimeister. 2022. “Quantum Computing.” Electronic Markets32(4):2525–36. doi: 10.1007/s12525-022-00570-y.

[30] González, Antonio. 2020. “Computación Cuántica y Aplicaciones.” Revista General de Marina278(4):635–40.

[31] Mosca, M., Stebila, D. (2016). Post-Quantum Cryptography: Current State and Open Problems. Proceedings of the 2016 IEEE International Conference on Communications (ICC 2016). https://doi.org/10.1109/ICC.2016.7510882

[32] Bernstein, D. J. (2017). Post-Quantum Cryptography. IEEE Security Privacy, 15(6), 9-12. https://doi.org/10.1109/MSP.2017.4211369