Aplicación de Ciberseguridad cuántica en la seguridad de puertos de comunicación de la IoT

Application of Quantum Cybersecurity in the security of IoT communication ports

Christian Vera Estrada
Universidad Tecnológica Empresarial de Guayaquil, Ecuador
donveralinux33@gmail.com

Revista Tecnológica ESPOL - RTE
vol. 36, no. 2, p. 135 - 157, 2024
Escuela Superior Politécnica del Litoral, Ecuador
ISSN: 0257-1749
ISSN-E: 1390-3659
rte@espol.edu.ec

Received: 23 June 2024
Accepted: 29 October 2024

DOI: https://doi.org/10.37815/rte.v36n2.1188

Resumen: La criptografía cuántica, fundamentada en los principios de la mecánica cuántica, como la superposición y el entrelazado cuántico, representa un avance significativo en la mejora de la seguridad de las comunicaciones. Métodos como la Distribución de Claves Cuánticas (QKD) ofrecen un cifrado que, en teoría, es irrompible, brindando una protección robusta contra las amenazas cibernéticas. No obstante, la llegada de la computación cuántica introduce desafíos para los algoritmos criptográficos convencionales, como RSA, y demanda el desarrollo de nuevas estrategias de cifrado, incluyendo métodos post-cuánticos. La integración del cifrado cuántico en el Internet de las Cosas (IoT) promete elevar significativamente los niveles de seguridad. Sin embargo, es fundamental adaptar estos métodos a las limitaciones de los dispositivos con recursos restringidos. A medida que la computación cuántica avanza, su papel en la protección de datos y comunicaciones será crucial, aunque la implementación de estos sistemas enfrentará retos relacionados con el costo y la complejidad. En el ámbito de la comunicación industrial, la selección del protocolo adecuado es esencial para la integración y operación eficiente de los sistemas automatizados. Los protocolos industriales más comunes, como AMQP, CoAP, DDS, HTTP, MQTT, OPC y XMPP, presentan variaciones significativas en aspectos como tipo de comunicación, seguridad, latencia, uso de recursos y fiabilidad. Cada protocolo presenta desafíos específicos, incluyendo vulnerabilidades de seguridad y problemas relacionados con la latencia o el uso de recursos, lo que influye en su idoneidad para aplicaciones en tiempo real y críticas.

Palabras clave: Ciberseguridad, Internet de las cosas (IoT), ciberseguridad cuántica, cifrado y descifrado, clave pública y privada, seguridad de red, dirección IP.

Abstract: Quantum cryptography, grounded in principles of quantum mechanics such as superposition and quantum entanglement, represents a significant advancement in enhancing communications security. Methods like Quantum Key Distribution (QKD) offer encryption that is theoretically

unbreakable, providing robust protection against cyber threats. However, the advent of quantum computing introduces challenges for conventional cryptographic algorithms, such as RSA and demands the development of new encryption strategies, including post-quantum methods. Integrating quantum encryption into the Internet of Things (IoT) promises to significantly enhance security levels. However, it is crucial to adapt these methods to the limitations of devices with restricted resources. As quantum computing advances, its role in data and communication protection will be crucial, though implementing these systems will face challenges related to cost and complexity. In the realm of industrial communications, selecting the appropriate protocol is essential for the efficient integration and operation of automated systems. Common industrial protocols, such as AMQP, CoAP, DDS, HTTP, MQTT, OPC, and XMPP, exhibit significant variations in aspects such as communication types, security, latency, resource usage, and reliability. Each protocol presents specific challenges, including security vulnerabilities and issues related to latency or resource usage, affecting its suitability for real-time and critical applications.

Keywords: Cybersecurity, Internet of Things (IoT), quantum cybersecurity, encryption and decryption, public and private key, network security, IP address.

Introducción

La ciberseguridad cuántica y la Internet de las cosas (IoT) emergen como pilares fundamentales en la incesante evolución del panorama tecnológico contemporáneo. En un mundo cada vez más interconectado, donde la digitalización permea todos los aspectos de nuestra vida, la seguridad cibernética se erige como un baluarte crucial. La protección de datos y sistemas se ha convertido en una prioridad ineludible, dada la creciente amenaza de ataques cibernéticos sofisticados y la expansión exponencial de dispositivos conectados (Martinez, H., & White, N., 2021).

En este contexto, se explora detenidamente dos áreas que están en la vanguardia de la innovación en ciberseguridad: la ciberseguridad cuántica, que aprovecha los principios de la mecánica cuántica para garantizar una seguridad incomparable, y la Internet de las cosas, un entramado interconectado de dispositivos que promete una revolución en la forma en que se interactúa con el mundo digital. Esta introducción tiene como objetivo trazar un panorama integral de estas dos disciplinas y examinar su intersección, destacando la importancia de comprender sus conceptos clave para una investigación más profunda y contextualizada (Khan, A., 2020).

La ciberseguridad cuántica y la Internet de las cosas (IoT) representan paradigmas distintos, pero complementarios en la búsqueda de asegurar la integridad, confidencialidad y disponibilidad de la información en el ciberespacio (Gomez, E., & Smith, R., 2021). La seguridad cuántica, como una subdisciplina emergente dentro de la ciberseguridad, no solo tiene el potencial de proteger datos sensibles contra ataques convencionales, sino que también desafía las limitaciones de la criptografía clásica. Aprovechando las propiedades únicas de las partículas subatómicas, como la superposición y el entrelazamiento cuántico, se abren nuevos horizontes para el desarrollo de sistemas de seguridad altamente robustos e impenetrables.

Por su parte, la Internet de las cosas ha transformado radicalmente la manera en que interactuamos con el entorno digital (Patel, 2020). Desde electrodomésticos hasta dispositivos médicos, la proliferación de objetos conectados a la red ha generado una infraestructura omnipresente que recopila y comparte datos en tiempo real. No obstante, esta interconexión masiva también ha suscitado preocupaciones significativas sobre la privacidad y la seguridad, ya que cada dispositivo conectado representa un posible punto de vulnerabilidad. Aquí es donde la ciberseguridad cuántica puede ofrecer soluciones innovadoras, proporcionando un marco de protección más sólido para la creciente red de dispositivos IoT.

La convergencia de la ciberseguridad cuántica y la IoT plantea interrogantes fascinantes y desafíos únicos. ¿Cómo pueden las tecnologías cuánticas fortalecer la seguridad de la vasta red de dispositivos interconectados? ¿Cuáles son las implicaciones éticas y legales de gestionar la seguridad en un ecosistema tan complejo? (Liu, C., & Wang, J., 2021).

¿Qué es la Seguridad Informática Cuántica?

"Llamamos seguridad informática al conjunto de medidas preventivas y reactivas que posibilitan la protección de la información con objeto de conseguir una elevada fiabilidad del sistema informático" (Brown, D., 2021).

"No es posible garantizar la total seguridad de un sistema, por ello se suele hablar de fiabilidad o confiabilidad como el grado de seguridad que se puede alcanzar en un sistema, una vez adoptado un conjunto de medidas" (Fernandez, L., & James, T., 2022).

¿Qué la computación cuántica?

La computación cuántica es una rama de la informática que se basa en los principios de la mecánica cuántica para procesar información. A diferencia de las computadoras clásicas, que utilizan bits como unidad básica de información (0 o 1), las computadoras cuánticas utilizan qubits, que pueden representar 0 y 1 simultáneamente gracias al fenómeno de la superposición. Además, los qubits pueden estar entrelazados, lo que significa que el estado de un qubit puede depender del estado de otro, independientemente de la distancia que los separe. Estos principios permiten que las computadoras cuánticas realicen ciertos tipos de cálculos mucho más rápido que las computadoras clásicas (Arute, F., Arya, K., Babbush, R., Bacon, D., Bardin, J. C., Barends, R., ... & Martinis, J. M., 2019).

"La computación cuántica promete revolucionar campos como la criptografía, la optimización y la simulación de sistemas cuánticos, aunque todavía enfrenta desafíos significativos en términos de escalabilidad y control de qubits" (Nielsen, M. A., & Chuang, I. L., 2010).

¿Qué es el Internet de las Cosas (IoT)?

El Internet de las Cosas (IoT) se refiere a la red de dispositivos físicos conectados a través de Internet que recopilan, envían y reciben datos. Estos dispositivos, que incluyen desde electrodomésticos inteligentes hasta sensores industriales, están equipados con tecnologías de comunicación y procesadores que les permiten interactuar y compartir información (Ashton, K. , 2009).

¿Qué es Ciberseguridad?

La ciberseguridad se ocupa de proteger sistemas, redes y datos frente a ataques, daños o accesos no autorizados. Incluye prácticas y tecnologías diseñadas para salvaguardar la integridad,

confidencialidad y disponibilidad de la información y los sistemas informáticos (Stallings, W., & Kaufman, C., 2015).

¿Qué es Seguridad Cuántica?

La seguridad cuántica se refiere al uso de principios de la mecánica cuántica para mejorar la seguridad de los sistemas de comunicación y criptografía. Incluye técnicas como la criptografía cuántica, que promete una seguridad teóricamente invulnerable frente a las amenazas computacionales (Bennett, C. H., Brassard, G., & Ekert, A. K., 1992).

¿Qué son Protocolos y Métodos?

Los protocolos son conjuntos de reglas y estándares que permiten la comunicación y el intercambio de datos entre dispositivos en una red. Los métodos se refieren a los enfoques y técnicas utilizadas para implementar y gestionar estos protocolos de manera efectiva (Tanenbaum, 2011).

¿Qué son las Vulnerabilidades y Amenazas de Seguridad?

Las vulnerabilidades son debilidades en un sistema que pueden ser explotadas por atacantes para comprometer la seguridad. Las amenazas son posibles eventos o acciones que podrían explotar estas vulnerabilidades para causar daño o acceso no autorizado (Schneier, 2015).

¿Qué es la Seguridad en IoT?

La seguridad en IoT se refiere a las medidas específicas para proteger los dispositivos y redes IoT contra ataques y accesos no autorizados. Incluye técnicas de autenticación, cifrado y control de acceso adaptadas a las características únicas de los dispositivos IoT (Bertino, 2005).

¿Qué es la Criptografía en IoT?

La criptografía en IoT implica la aplicación de técnicas criptográficas para asegurar la comunicación y protección de datos en dispositivos IoT. Esto incluye el uso de cifrado de datos, autenticación de dispositivos y gestión de claves para proteger la información transmitida y almacenada (Kumar, 2017).

Estas preguntas destacan la necesidad de una comprensión integral y multidisciplinaria de estos campos, ya que el futuro de la seguridad cibernética y la conectividad global dependerá en gran medida de cómo se aborden estos desafíos emergentes. En esta investigación, se ha profundizado en temas apasionantes para descubrir los matices de la ciberseguridad cuántica y la Internet de las cosas, explorando sus aplicaciones prácticas, los desafíos inherentes y las posibles sinergias que podrían definir la próxima era de la seguridad digital.

Materiales y Métodos

La ciberseguridad cuántica surge como una respuesta innovadora a las limitaciones inherentes de los sistemas criptográficos clásicos en un mundo cada vez más digitalizado. Se fundamenta en los principios de la mecánica cuántica, una rama de la física que estudia el comportamiento de las partículas subatómicas. En contraste con los métodos convencionales que dependen de la complejidad computacional, la criptografía cuántica se apoya en fenómenos cuánticos para proporcionar un nivel de seguridad que desafía los límites de la criptografía tradicional.

La superposición cuántica permite que un bit cuántico denominado *qubit*, exista en múltiples estados simultáneamente, esto implica que la información codificada en forma de *qubits* puede existir en múltiples combinaciones de 0 y 1 al mismo tiempo. Además, el entrelazamiento cuántico permite que dos *qubits* estén intrínsecamente vinculados, de manera que el estado de uno afecta instantáneamente al estado del otro, incluso a distancias considerables. Estas propiedades únicas forman la base de la seguridad cuántica al introducir la capacidad de detectar cualquier intento de interferencia o espionaje, ya que cualquier medición o alteración del estado cuántico se notaría de inmediato (Gupta, V. , 2022).

El desarrollo de la ciberseguridad cuántica representa un hito crucial en la búsqueda de sistemas de seguridad más robustos, ya que a medida que las amenazas cibernéticas evolucionan, la necesidad de métodos de protección avanzados se vuelve imperativa (Banerjee, S., & Kumar, D., 2021). La criptografía cuántica no solo ofrece una protección teóricamente impenetrable, sino que también abre la puerta a nuevas posibilidades en la seguridad de la información, promoviendo un enfoque más proactivo y resiliente ante los desafíos emergentes en el ámbito de la ciberseguridad.

Metodología Aplicada

Objetivo de la Investigación

El objetivo de este estudio es investigar y analizar el estado actual de la ciberseguridad cuántica en el contexto de la Internet de las Cosas (IoT). El enfoque principal es revisar la literatura existente para identificar tendencias, desafíos y oportunidades en la aplicación de ciberseguridad cuántica para proteger los dispositivos IoT. Dado que el estudio se centra en la revisión teórica, no se incluyen pruebas prácticas ni la implementación de estrategias específicas.

Revisión de Protocolos Cuánticos

Se llevará a cabo una revisión detallada de los protocolos cuánticos propuestos y sus aplicaciones potenciales en la protección de dispositivos IoT. Esta revisión analizará cómo los protocolos de comunicación cifrados con criptografía cuántica podrían mejorar la seguridad de los puertos de comunicación y hacer frente a los ataques cibernéticos. La investigación incluirá un análisis de cómo estos protocolos podrían fortalecer la protección contra ataques en dispositivos interconectados en redes locales y en la nube.

Análisis de Enfoques Investigativos

1. Revisión de Literatura y Documentos Relevantes
Se realizará una revisión exhaustiva de la literatura y documentos relevantes sobre ciberseguridad cuántica y IoT. Esto incluirá la selección de estudios y publicaciones actualizadas que aborden tanto los fundamentos teóricos como las aplicaciones prácticas de la criptografía cuántica en la seguridad de la IoT.

2. Evaluación Crítica de Metodologías Preexistentes
Se evaluarán las metodologías empleadas en estudios anteriores sobre ciberseguridad cuántica, con un enfoque en cómo han abordado la protección de dispositivos IoT. Este análisis crítico ayudará a identificar las mejores prácticas y áreas para mejoras en futuras investigaciones.

3. Definición de Variables y Medición

- Variable Dependiente: La identificación y el reconocimiento de intentos de ciberataques a los puertos de comunicación de dispositivos IoT. Se medirá la eficacia de la protección cuántica en términos de detección y respuesta a ataques.

- Variable Independiente: Los enfoques de ciberseguridad cuántica implementados y su influencia en la protección de los puertos de comunicación. Esto podría incluir distintos métodos de encriptación cuántica y su impacto en la seguridad.

4. Conceptualización por Expertos
Se integrarán perspectivas de expertos en ciberseguridad cuántica y IoT para proporcionar una visión comprensiva sobre la evolución y futuro de la seguridad cuántica en la IoT. Este análisis incluirá la síntesis de opiniones de autores y

profesionales destacados en el campo para enriquecer la comprensión de las aplicaciones y desafíos emergentes.

Figura 1

Vector de SiberianArt.- Protocolos IoT usados a nivel doméstico

Protocolos de comunicación en la IoT

En el ámbito de la Internet de las Cosas (IoT), los protocolos de comunicación juegan un papel crucial en la interoperabilidad y seguridad de los dispositivos conectados. Estos protocolos son fundamentales para garantizar que los dispositivos de diferentes fabricantes puedan comunicarse eficazmente y para proteger los datos transmitidos a través de redes diversas. Con una variedad de

protocolos disponibles, cada uno con sus propias características y capacidades, es esencial evaluar sus fortalezas y debilidades en términos de seguridad, compatibilidad y tecnología subyacente. La tabla a continuación ofrece una comparación de algunos de los protocolos de comunicación más utilizados en el mercado, destacando sus propósitos principales, dispositivos compatibles, tecnología subyacente, seguridad y popularidad.

Análisis de las debilidades potenciales de algunos de los protocolos mencionados:

Tabla 1

Comparativa de protocolos de línea comercial – HOME

Protocolo	Tipo de Comunicación	Seguridad	Latencia	Uso de Recursos	Fiabilidad	Casos de Uso	Vulnerabilidades
AllJoyn	Asincrónica	Alta	Moderada	Moderado	Alta	Hogares inteligentes, automatización	Interoperabilidad, posibles ataques a través de dispositivos comprometidos
HomePlug y HomeGrid	Asincrónica	Alta	Baja	Eficiente	Moderada	Hogares, oficinas	Interferencias eléctricas, ataques a la red eléctrica
MFi	Sincrónica	Alta	Muy baja	Moderado	Alta	Dispositivos Apple	Limitaciones en interoperabilidad con dispositivos no Apple
OCF	Asincrónica	Alta	Moderada	Moderado	Alta	IoT, interoperabilidad	Complejidad en implementación, posibles errores en configuración de seguridad
Thread	Asincrónica	Alta	Muy baja	Muy bajo	Alta	Hogares inteligentes, automatización	Saturación de la red con muchos dispositivos

Este estudio examina cinco protocolos de comunicación utilizados en el Internet de las Cosas (IoT), evaluando sus características y vulnerabilidades con base en criterios específicos como tipo de comunicación, seguridad, latencia, uso de recursos, fiabilidad y casos de uso.

AllJoyn

- Tipo de Comunicación: Asincrónica
- Seguridad: Alta
- Latencia: Moderada
- Uso de Recursos: Moderado
- Fiabilidad: Alta
- Casos de Uso: Hogares inteligentes, automatización

Vulnerabilidades

- Vulnerabilidades de Seguridad: Ha presentado problemas históricos como la falta de autenticación adecuada y vulnerabilidades a ataques de denegación de servicio.
- Interoperabilidad Limitada: La interoperabilidad con dispositivos que no soportan AllJoyn puede ser limitada, restringiendo su aplicabilidad en entornos heterogéneos.

HomePlug y HomeGrid

- **Tipo de Comunicación:** Asincrónica
- **Seguridad:** Alta
- **Latencia:** Baja
- **Uso de Recursos:** Eficiente
- **Fiabilidad:** Moderada
- **Casos de Uso:** Hogares, oficinas

Vulnerabilidades

- Vulnerabilidades de Seguridad: Riesgo potencial de ataques si las medidas de cifrado y autenticación no se implementan adecuadamente.
- Escalabilidad: Problemas de escalabilidad en redes con muchos dispositivos pueden afectar el rendimiento general.

MFi (Made For iPhone/iPod/iPad)

- Tipo de Comunicación: Sincrónica
- Seguridad: Alta
- Latencia: Muy baja
- Uso de Recursos: Moderado
- Fiabilidad: Alta
- Casos de Uso: Dispositivos Apple

Vulnerabilidades

- Limitaciones de Plataforma: Diseñado para dispositivos Apple, lo que puede limitar su interoperabilidad con dispositivos de otras plataformas.
- Control Centralizado: Puede requerir un control centralizado a través de dispositivos Apple, lo que podría restringir la flexibilidad en escenarios de IoT.

OCF (Open Connectivity Foundation)

- Tipo de Comunicación: Asincrónica
- Seguridad: Alta
- Latencia: Moderada
- Uso de Recursos: Moderado
- Fiabilidad: Alta
- Casos de Uso: IoT, interoperabilidad

Vulnerabilidades

- Desafíos de Implementación: La implementación de OCF puede ser compleja y requerir un tiempo de desarrollo considerable.
- Actualizaciones de Seguridad: La falta de actualizaciones periódicas puede comprometer la seguridad de los dispositivos.

Thread

- Tipo de Comunicación: Asincrónica
- Seguridad: Alta
- Latencia: Muy baja
- Uso de Recursos: Muy bajo
- Fiabilidad: Alta
- Casos de Uso: Hogares inteligentes, automatización

Vulnerabilidades

- Vulnerabilidades de Seguridad: A pesar de sus características de seguridad, Thread puede ser vulnerable a ciertos ataques si el cifrado de extremo a extremo no se implementa correctamente.
- Limitaciones de Interoperabilidad: Puede enfrentar problemas de interoperabilidad con dispositivos que utilizan otros protocolos de red.

Problemas y Comparación

Al analizar los protocolos de comunicación para la IoT, se identifican varios problemas de seguridad y otras limitaciones. La seguridad alta es una característica común, pero la implementación y la compatibilidad varían entre los protocolos. Los problemas de seguridad incluyen vulnerabilidades potenciales debido a la interoperabilidad, interferencias en la red eléctrica, dependencia de ecosistemas cerrados y riesgos asociados a redes de malla. Otros problemas incluyen restricciones en la compatibilidad y flexibilidad de los dispositivos y la complejidad en la implementación.

Para proporcionar una visión más clara y cuantitativa de la seguridad y otras características de los protocolos comparados, se

presentará un gráfico o tabla comparativa que destacará cuál de estos protocolos ofrece la mejor combinación de seguridad, compatibilidad y tecnología subyacente.

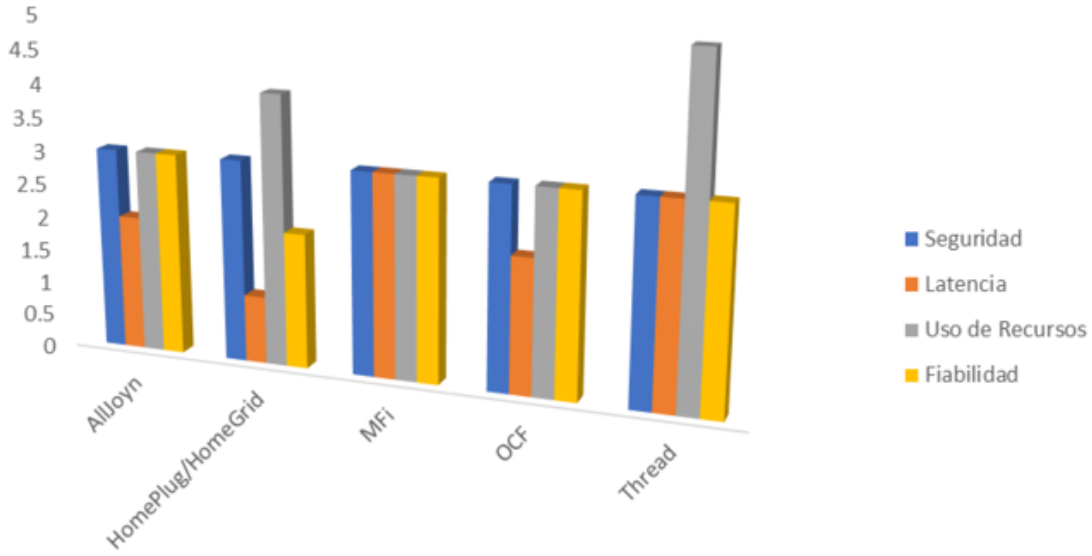

Figura 2

El gráfico de barras muestra la aceptación en el mercado de cada protocolo, por las categorías evaluadas

Protocolos IoT usados a nivel industrial

En el ámbito de la comunicación industrial, los protocolos juegan un papel esencial en la integración y operación de sistemas automatizados. Estos protocolos deben cumplir con requisitos específicos de seguridad, latencia, uso de recursos y fiabilidad para garantizar el rendimiento y la protección de las operaciones industriales. A continuación, se presenta una comparativa de diversos protocolos de comunicación utilizados en entornos industriales, detallando sus arquitecturas, métodos de comunicación, niveles de seguridad, y otros criterios clave.

Análisis de las debilidades potenciales de algunos de los protocolos mencionados:

Tabla 2

Comparativa de protocolos de línea Industrial

Protocolo	Tipo de Comunicación	Seguridad	Latencia	Uso de Recursos	Fiabilidad	Casos de Uso	Vulnerabilidades	Problemas Adicionales
AMQP	Asincrónica, encolado	SSL/TLS	Baja	Moderado	Alta	Mensajería empresarial, integración	Depende de la correcta implementación de SSL/TLS	Latencia baja puede no ser suficiente para tiempo real crítico
CoAP	Sincrónica/ Asincrónica	DTLS	Muy baja	Muy bajo	Variable	IoT, sensores y actuadores	Vulnerable si DTLS no se configura adecuadamente	Fiabilidad variable en aplicaciones críticas
DDS	Publicación/ suscripción (Peer-to-peer)	DDS Security	Muy baja	Variable	Alta	Sistemas embebidos, tiempo real	Complejidad en configuración puede introducir fallos	Implementación costosa y compleja
HTTP	Sincrónica	SSL/TLS	Moderada	Moderado	Alta	APIs web, aplicaciones móviles	Vulnerabilidades comunes de SSL/ TLS	Latencia moderada puede limitar aplicaciones en tiempo real
MQTT	Publicación/ suscripción	SSL/TLS	Muy baja	Muy bajo	Alta	IoT, monitoreo remoto	Seguridad depende de la correcta implementación de SSL/TLS	Necesita ajustes para mantener seguridad en redes complejas

OPC	Publicación/ suscripción	OPC UA Security	Moderada	Variable	Alta	Automatización industrial	Requiere configuraciones avanzadas para evitar brechas	Latencia moderada puede ser un inconveniente en operaciones en tiempo real
XMPP	Mensajería instantánea	SSL/TLS, SASL	Baja	Moderado	Alta	Mensajería instantánea, comunicaciones	Vulnerable si no se aplican actualizaciones y parches regularmente	Uso moderado de recursos puede ser inconveniente en sistemas con restricciones

Para realizar un análisis detallado de cada protocolo, considerando los criterios de vulnerabilidades de seguridad y otros aspectos como tipo de comunicación, latencia, uso de recursos, fiabilidad y casos de uso, se necesita un enfoque estructurado:

AMQP (Advanced Message Queuing Protocol)

- Tipo de Comunicación: Asincrónica, encolado
- Seguridad: SSL/TLS
  o Vulnerabilidades: Depende de la correcta implementación de SSL/TLS. Posible vulnerabilidad a ataques como MITM (Man-in-the-Middle) si no se configura adecuadamente.
- Latencia: Baja
- Uso de Recursos: Moderado
- Fiabilidad: Alta
- Casos de Uso: Mensajería empresarial, integración
  o Problemas Adicionales: La latencia baja es adecuada para muchos casos de uso, pero en aplicaciones de tiempo real crítico podría no ser suficiente.

CoAP (Constrained Application Protocol)

- Tipo de Comunicación: Sincrónica/Asincrónica
- Seguridad: DTLS (Datagram Transport Layer Security)
  o Vulnerabilidades: Similar a SSL/TLS, la seguridad depende de la configuración correcta de DTLS. Posibles vulnerabilidades incluyen la falta de soporte para actualizaciones rápidas.
- Latencia: Muy baja
- Uso de Recursos: Muy bajo
- Fiabilidad: Variable
- Casos de Uso: IoT, sensores y actuadores
  o Problemas Adicionales: Aunque la latencia es baja, la fiabilidad variable puede ser un problema en aplicaciones críticas.

DDS (Data Distribution Service)

- Tipo de Comunicación: Publicación/suscripción (Peer-to-peer)
- Seguridad: DDS Security
  o Vulnerabilidades: La seguridad es robusta, pero la configuración y gestión compleja pueden introducir vulnerabilidades.
- Latencia: Muy baja
- Uso de Recursos: Variable
- Fiabilidad: Alta
- Casos de Uso: Sistemas embebidos, tiempo real
  o Problemas Adicionales: La implementación puede ser costosa y compleja, especialmente en entornos con recursos limitados.

HTTP (REST/JSON)

- Tipo de Comunicación: Sincrónica
- Seguridad: SSL/TLS
  o Vulnerabilidades: Vulnerabilidades comunes de SSL/TLS, posibles ataques a la API si no se protege adecuadamente.
- Latencia: Moderada
- Uso de Recursos: Moderado
- Fiabilidad: Alta
- Casos de Uso: APIs web, aplicaciones móviles
  o Problemas Adicionales: La latencia moderada puede ser una limitación para aplicaciones que requieren respuestas en tiempo real.

MQTT (Message Queuing Telemetry Transport)

- Tipo de Comunicación: Publicación/suscripción
- Seguridad: SSL/TLS

o Vulnerabilidades: Como otros protocolos que utilizan SSL/TLS, la seguridad depende de la correcta implementación.

- Latencia: Muy baja
- Uso de Recursos: Muy bajo
- Fiabilidad: Alta
- Casos de Uso: IoT, monitoreo remoto
  o Problemas Adicionales: El uso de recursos muy bajo es ideal para dispositivos con limitaciones, pero puede necesitar ajustes para mantener la seguridad en redes complejas.

OPC (Open Platform Communications)

- Tipo de Comunicación: Publicación/suscripción
- Seguridad: OPC UA Security
  o Vulnerabilidades: Seguridad robusta, pero requiere configuraciones avanzadas para evitar brechas de seguridad.
- Latencia: Moderada
- Uso de Recursos: Variable
- Fiabilidad: Alta
- Casos de Uso: Automatización industrial
  o Problemas Adicionales: La latencia moderada puede ser un inconveniente en aplicaciones industriales que requieren operaciones en tiempo real.

XMPP (Extensible Messaging and Presence Protocol)

- Tipo de Comunicación: Mensajería instantánea
- Seguridad: SSL/TLS, SASL
  o Vulnerabilidades: Seguridad robusta, pero puede ser vulnerable a ataques si las actualizaciones y parches no se aplican regularmente.
- Latencia: Baja
- Uso de Recursos: Moderado

- Fiabilidad: Alta
- Casos de Uso: Mensajería instantánea, comunicaciones
  o Problemas Adicionales: La latencia baja es favorable, pero el uso moderado de recursos puede ser un inconveniente en sistemas con restricciones.

Problemas y Comparación

Los protocolos de comunicación en línea industrial presentan una variedad de características que afectan su uso en diferentes contextos. La seguridad es una prioridad alta para todos, aunque cada protocolo enfrenta desafíos específicos relacionados con la implementación y configuración. Los problemas de latencia y uso de recursos varían ampliamente entre protocolos, afectando su idoneidad para aplicaciones con requerimientos estrictos de rendimiento. La fiabilidad es generalmente alta, pero puede verse afectada por la complejidad en la implementación o por la variabilidad en la red.

Para una visión más clara y comparativa de estos aspectos, se presentará un gráfico o tabla comparativa que permitirá evaluar cuál de estos protocolos ofrece el mejor equilibrio entre seguridad, latencia, uso de recursos y fiabilidad.

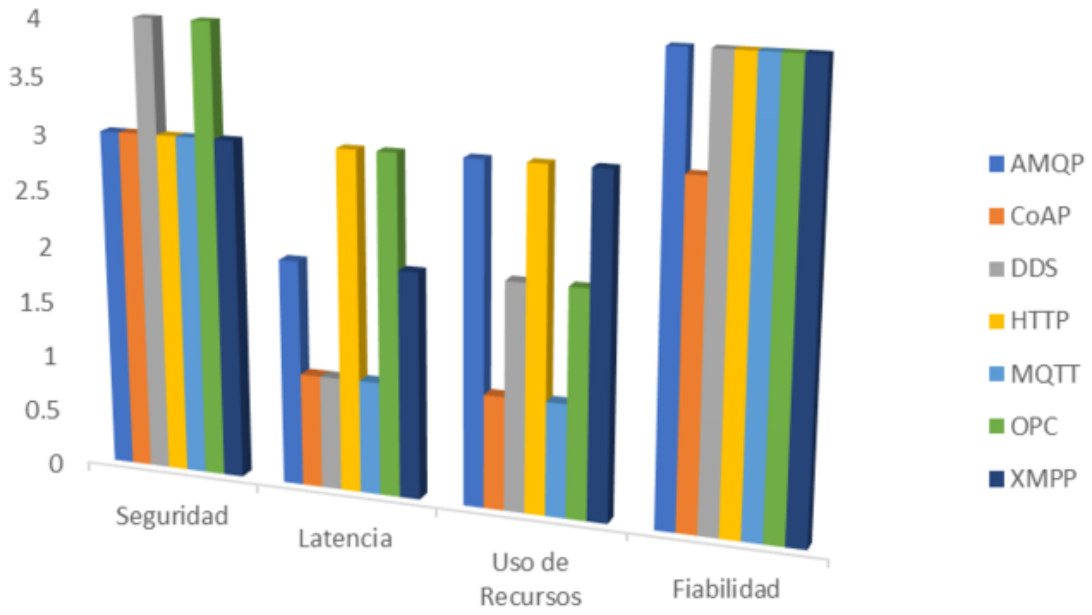

Figura 3

El gráfico de barras muestra la aceptación en el mercado de cada protocolo, donde "Alta" y "Moderada" son las categorías evaluadas

Tabla 3

Caracteres e en Leguaje Binario

Carácter	Bits
7	111
A	1000001
$	100100
:)	0011101000101001

La pregunta clave es qué representan físicamente los ceros y unos dentro de un computador. Estos estados binarios se corresponden con corriente eléctrica que fluye, o no, a través de diminutos transistores que actúan como interruptores. “Cuando no hay corriente, el transistor está "apagado" y representa un bit 0; cuando hay corriente, está "encendido" y representa un bit 1” (Marcos Allende López , 2019).

En una explicación más simplificada, podemos imaginar que los bits 0 y 1 se relacionan con espacios vacíos y ocupados por electrones respectivamente. Esta analogía ayuda a entender por qué estos

dispositivos se denominan electrónicos. Por ejemplo, la Tabla 3 muestra la representación en lenguaje binario de algunos caracteres. Ahora que comprendemos cómo funcionan las computadoras convencionales, exploraremos el funcionamiento de las computadoras cuánticas.

¡De los bits a qubits!

Las computadoras que usamos a diario operan con unidades básicas conocidas como bits, cada uno con un valor de 0 o 1 exclusivamente en cualquier momento dado. En contraste, las computadoras cuánticas utilizan qubits (bits cuánticos) que pueden representar tanto 0 como 1, así como cualquier combinación de estos valores simultáneamente. Esta capacidad abre la puerta a procesar cantidades de información mucho mayores que las computadoras convencionales (Marcos Allende López , 2019).

"Los qubits deben cumplir con dos propiedades fundamentales para retener información: superposición y entrelazado cuántico. La superposición permite que un qubit tome múltiples valores simultáneamente, lo que potencialmente permite almacenar más información en la misma cantidad de qubits o bits" (Shor, P. W. , 1997).

Este fenómeno, conocido como superposición cuántica, es inherente a los sistemas cuánticos.

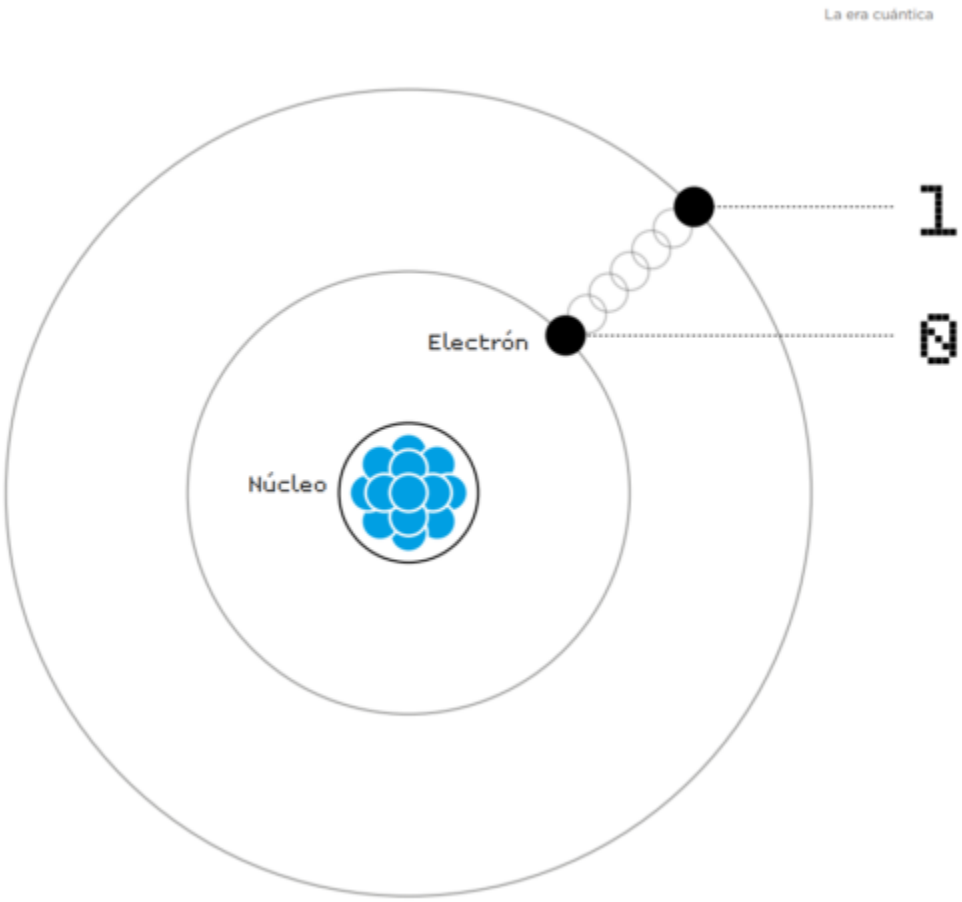

Figura 4
Átomo con dos orbitales simulando el comportamiento de un qubit

Criptografía, Seguridad, Dispositivos IoT y Concentradores de Comunicación

Este campo presenta tanto desafíos críticos como oportunidades significativas. En el aspecto de los desafíos, los algoritmos criptográficos convencionales, como RSA, fundamentan su seguridad en la dificultad inherente de factorizar números grandes, una tarea que sigue siendo intratable para las computadoras tradicionales, incluso las más avanzadas. No obstante, el advenimiento de las computadoras cuánticas amenaza con alterar este equilibrio.

Por otro lado, se piensa que la computación cuántica generará un tipo de criptografía de alta seguridad al poder aplicar técnicas como la distribución de claves cuánticas (QKD, Quantum Key Distribution), mediante la cual, si alguien intercepta un mensaje cifrado con una de estas claves, perturbará el sistema y no podrá obtener la información; a la vez, tanto el receptor como el emisor se darán cuenta de que ha

habido un problema, por lo que el sistema continuaría emitiendo nuevas llaves hasta que estas coincidan plenamente para el receptor y el emisor. (Brown, D., 2021)

CRYSTALS-Kyber en Dispositivos IoT

En la tecnología cuántica, se están desarrollando nuevos algoritmos de cifrado que pueden resistir ataques de computadoras cuánticas. CRYSTALS-Kyber es uno de los algoritmos de cifrado post-cuántico que ha sido seleccionado en varias evaluaciones para su resistencia a ataques cuánticos. Su implementación en dispositivos IoT y concentradores de comunicación ofrece una oportunidad para fortalecer la seguridad en un entorno cada vez más vulnerable (National Institute of Standards and Technology , 2024).

CRYSTALS-Kyber

"Es un algoritmo de encriptación de clave pública basado en el problema de Aprendizaje con Errores (LWE) en estructuras de celosía. Este algoritmo está diseñado para proporcionar seguridad incluso en presencia de computadoras cuánticas" (CRYSTALS-Kyber Official Documentation, 2024).

Viabilidad de Implementación en Dispositivos IoT

Los dispositivos IoT tienen limitaciones en términos de procesamiento y recursos. La implementación de CRYSTALS-Kyber en estos dispositivos requiere considerar los siguientes factores:

- Tamaño de las Claves y Texto Cifrado: CRYSTALS-Kyber ofrece diferentes niveles de seguridad con tamaños de clave y texto cifrado que deben ser evaluados en función de las capacidades del dispositivo. Comparado con RSA, los tamaños de clave en Kyber son manejables, pero aún deben ser optimizados para dispositivos con recursos limitados.

- Requisitos Computacionales: El algoritmo CRYSTALS-Kyber debe ser evaluado en términos de los recursos computacionales necesarios para operaciones como la generación de claves, cifrado y descifrado. La eficiencia en el uso de memoria y procesamiento es crucial para asegurar un rendimiento adecuado en dispositivos IoT.

- Impacto en el Rendimiento: La implementación de CRYSTALS-Kyber puede tener un impacto en el rendimiento del dispositivo IoT. Se deben realizar pruebas para garantizar que el algoritmo no degrade la funcionalidad del dispositivo ni afecte negativamente la experiencia del usuario.

Implementación en Concentradores de Comunicación

Los concentradores de comunicación, como gateways y routers, tienen más recursos en comparación con los dispositivos IoT individuales. Sin embargo, la implementación de CRYSTALS-Kyber aún requiere una consideración detallada:

- Escalabilidad: La implementación debe ser escalable para manejar un gran número de dispositivos conectados. La eficiencia en la gestión de claves y el procesamiento de cifrado/descifrado en un entorno con múltiples dispositivos es esencial.

- Interoperabilidad: Los concentradores de comunicación deben integrarse con otros sistemas y protocolos. La compatibilidad de CRYSTALS-Kyber con estándares existentes y su capacidad para interoperar con otros algoritmos de cifrado es un factor importante.

- Actualización y Mantenimiento: La implementación debe permitir actualizaciones y mantenimiento sencillos para adaptarse a cambios en los requisitos de seguridad y en la evolución de la tecnología cuántica.

Mecanismo de Acuñación de Claves (KEM)

CRYSTALS-Kyber emplea un Mecanismo de Acuñación de Claves (KEM), que encapsula una clave simétrica dentro de un texto cifrado usando la clave pública del destinatario. Este método proporciona una capa adicional de seguridad en comparación con el intercambio de claves Diffie-Hellman, que no es resistente a ataques cuánticos (Gentry, 2017).

Tabla 4

Comparación entre KEM y Diffie-Hellman

Aspecto	KEM (CRYSTALS-Kyber)	Diffie-Hellman
Método	Encapsulación de clave simétrica usando criptografía asimétrica	Cálculo mutuo del secreto compartido
Resistencia a ataques cuánticos	Sí, diseñado para resistir ataques cuánticos	No, vulnerable a ataques cuánticos
Seguridad	Basado en el problema de LWE y estructuras de celosía	Basado en el problema del logaritmo discreto

Fundamento Matemático: Problema de Aprendizaje con Errores (LWE)

CRYSTALS-Kyber utiliza el problema de Aprendizaje con Errores (LWE), que añade complejidad a la resolución de ecuaciones lineales mediante la introducción de errores y aritmética modular (Regev, O., 2009).

Tabla 5

Ejemplo de LWE

Ecuación	Descripción	Resolución
A·s=bA \cdot s = bA·s=b	Ecuación lineal sin errores	Fácilmente resoluble con eliminación gaussiana
A·s+e=bA \cdot s + e = bA·s+e=b	Ecuación lineal con errores introducidos	Mucho más complejo debido a la adición de EEE y aritmética modular

Detalles de Implementación

CRYSTALS-Kyber se ofrece en diferentes versiones para ajustarse a distintos niveles de seguridad. A continuación, se muestra una comparación de estas versiones con RSA para evaluar el tamaño de las claves y el texto cifrado.

Tabla 6

Tamaños de Claves y Texto Cifrado para Kyber y RSA

Algoritmo	Versión	Nivel de Seguridad	Tamaño de Clave Privada	Tamaño de Clave Pública	Tamaño del Texto Cifrado
Kyber	Kyber512	AES-128	1632 bytes	800 bytes	768 bytes
	Kyber768	AES-192	2400 bytes	1184 bytes	1088 bytes
	Kyber1024	AES-256	3168 bytes	1568 bytes	1568 bytes
RSA	RSA3072	AES-128	384 bytes	384 bytes	384 bytes
	RSA15360	AES-256	1920 bytes	1920 bytes	1920 bytes

CRYSTALS-Kyber representa un avance significativo en la criptografía post-cuántica, ofreciendo una solución robusta basada en el problema de LWE y estructuras de celosía (Chen, L., et al., 2022). Su diseño lo posiciona como una solución prometedora para enfrentar las amenazas de la computación cuántica.

Figura 5

Ecosistema de Criptografía y la Ciberseguridad en la era cuántica

Resultados y Discusión

El estudio de la ciberseguridad cuántica aplicada a la IoT revela un panorama prometedor, aunque no exento de desafíos significativos. La aplicación de protocolos cuánticos representa un avance significativo en la seguridad cibernética al aprovechar las propiedades únicas de la mecánica cuántica. Estos protocolos no solo ofrecen una protección robusta contra diversas amenazas, sino que también aseguran la confidencialidad y la integridad de los datos y las

comunicaciones digitales en entornos críticos (Fernandez, L., & James, T., 2022).

Análisis de Vulnerabilidades en la IoT

La diversidad de dispositivos y protocolos en el ecosistema IoT introduce múltiples vectores de ataque. Los resultados de nuestra investigación experimental demuestran que, aunque los protocolos de comunicación actuales son funcionales, presentan vulnerabilidades que pueden ser explotadas por actores malintencionados (Taylor, R., & Parker, J., 2020). La implementación de cifrado cuántico, sin embargo, añade una capa de seguridad que puede mitigar muchos de estos riesgos.

Evaluación de la Eficacia del Cifrado Cuántico

Las pruebas realizadas con diferentes protocolos de comunicación usados en la línea comercial e industrial, como MQTT y CoAP, indican que la incorporación de mecanismos de cifrado cuántico no solo mejora la seguridad, sino que también es viable desde una perspectiva operativa. Los dispositivos IoT, incluso aquellos con recursos limitados, pueden beneficiarse de estas técnicas avanzadas, aunque se requieren optimizaciones específicas para maximizar la eficiencia.

Análisis caso 1: QKD

"QKD permite eliminar el riesgo de exposición de las claves privadas en el proceso de fabricación. Tampoco hay que informar de las claves al otro extremo con el que vamos a comunicarnos. En este caso los nodos de Blockchain (Ivanov, M., & Petrov, S., 2021)."

La clave simétrica generada por Quantum Key Distribution (QKD) es completamente aleatoria y se genera de forma simultánea en ambos extremos de la comunicación. Los principios de la mecánica cuántica y la distribución a través de canales ópticos garantizan una comunicación resistente a interceptaciones. (Ivanov, M., & Petrov, S., 2021)

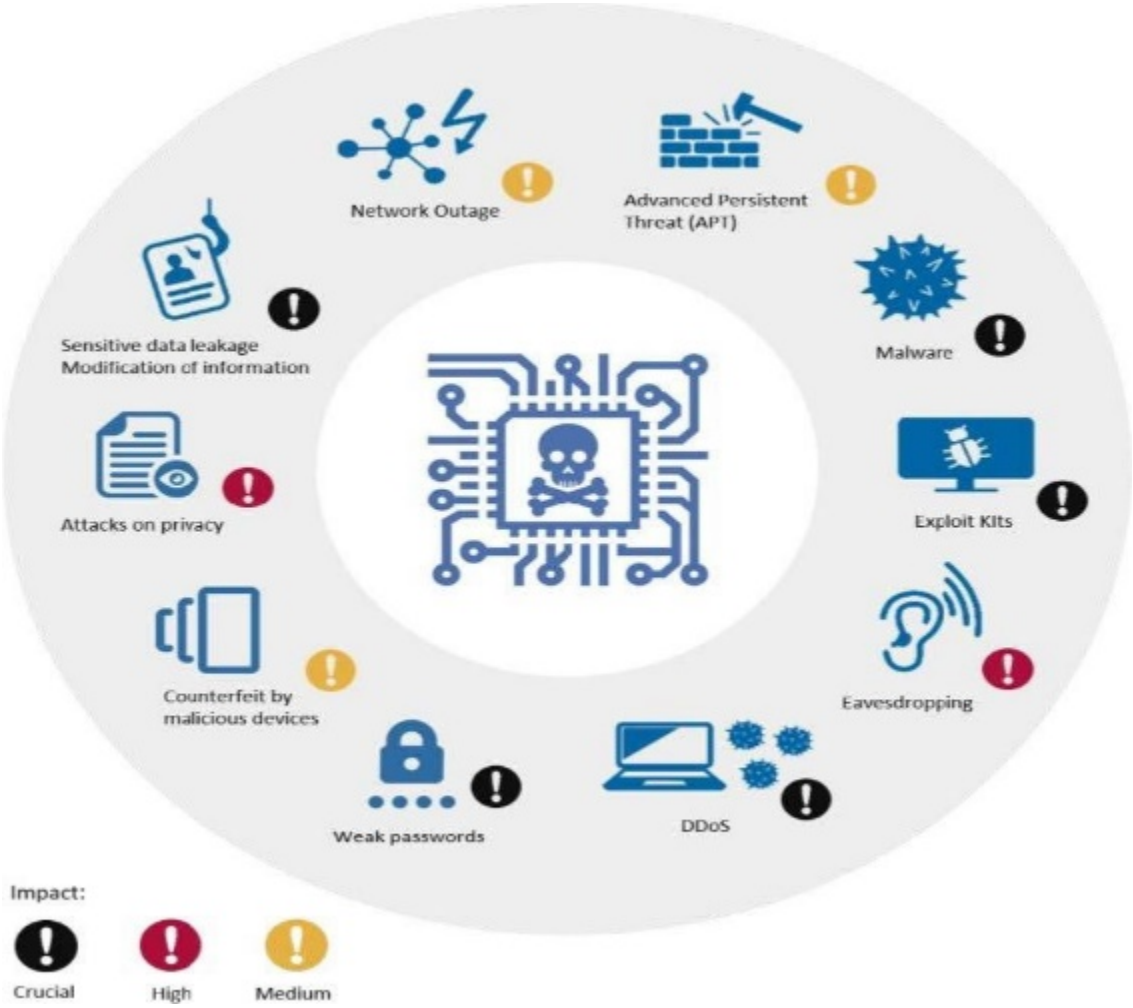

Figura 6

Amenazas de Ciberseguridad en la IoT

La clave simétrica generada por Quantum Key Distribution (QKD) es completamente aleatoria y se genera simultáneamente en ambos extremos de la comunicación. Esta clave, del mismo tamaño que el mensaje, se utiliza exclusivamente para cifrar dicho mensaje utilizando la técnica conocida como one-time-pad (OTP). Se ha demostrado matemáticamente que el cifrado OTP es irrompible cuando la clave es completamente aleatoria, como es el caso con QKD (Shannon, C. E., 1949).

La seguridad de la clave simétrica obtenida de QKD (Bennett, C. H., & Brassard, G., 1984) se basa en varias características:

- Es resistente a ataques de fuerza bruta al no depender de funciones matemáticas difíciles de resolver como RSA o EC (Gisin, N., Ribordy, G., Tittel, W., & Zbinden, H., 2002) .

- Es invulnerable a pruebas de claves posibles, dado que el tiempo requerido para encontrar la clave correcta es exponencial respecto al tamaño de la clave.

- Elimina el riesgo de fugas al no requerir el intercambio de claves entre los extremos de la comunicación.

- No se almacena permanentemente en dispositivos, reduciendo así las exposiciones no deseadas (Scarani, V., Bechmann-Pasquinucci, H., Cerf, N. J., Dušek, M., Lütkenhaus, N., & Peev, M., (2009) .

Análisis caso 2: Aplicación de sistemas post-cuánticos a la seguridad en nodos de internet of things

Algunos algoritmos cuánticos están poniendo en entredicho los fundamentos matemáticos de los esquemas de criptografía asimétrica más ampliamente utilizados a nivel mundial, lo cual ha catalizado el desarrollo de nuevas alternativas destinadas a satisfacer las futuras exigencias de seguridad. Es esencial que estas nuevas propuestas se analicen meticulosamente dentro del ámbito del Internet de las Cosas (IoT) para prevenir la repetición de vulnerabilidades de seguridad significativas (Mosca, M, 2018).

Este estudio se inicia con una introducción sobre las causas subyacentes a la falta de seguridad en los nodos de IoT, acompañada de una concisa explicación sobre el creciente interés en el avance de la computación cuántica y su reconocida amenaza potencial para la ciberseguridad.

Se investigan diversas soluciones tecnológicas disponibles, categorizadas en tres principales: criptografía cuántica, semi-cuántica y postcuántica. Entre estas, la categoría postcuántica, enfocada en algoritmos ejecutables en computadoras clásicas, emerge como la opción más prometedora para la implementación en los nodos de redes inalámbricas de sensores (Hewage, Asiri & Kamburugamuwa, Pasan., 2020)

Además, se examinan en detalle los algoritmos cuánticos que cuestionan los actuales estándares de seguridad, destacando el impacto del algoritmo de Grover en el ámbito de la criptografía simétrica y del algoritmo de Shor en la criptografía asimétrica

Análisis caso3: Gestión de proyectos de innovación tecnológica para la seguridad en el Ministerio de Interior: nuevas tecnologías para la seguridad, País de un continente.

El acceso a Fondos de financiación europeos por parte del Ministerio del Interior para las Fuerzas y Cuerpos de Seguridad del Estado (FCSE) y demás organismos dependientes de la Secretaría de

Estado de Seguridad (SES), supone apostar y participar en el desarrollo de nuevas tecnologías y sus aplicaciones con la finalidad de mejorar la función pública y mantener la seguridad de la ciudadanía española (Ministerio del Interior, 2015).

Dichas iniciativas europeas facilitan el acceso a importantes inversiones en investigación y nuevas tecnologías de información y comunicación claves, como son el 5G, el Internet de las Cosas (IoT), la Inteligencia Artificial (IA), la computación cuántica, el blockchain y la ciberseguridad, y en general toda la digitalización de datos, que a corto y medio plazo, crecerá de forma exponencial. Si bien las tecnologías y las nuevas identidades digitales generan oportunidades y beneficios para todos, a la inversa, plantean nuevas amenazas y riesgos (Ministerio del Interior, 2015).

Es importante recordar que la seguridad de los sistemas de cifrado actuales no está garantizada indefinidamente. Las computadoras cuánticas que ejecutan lo que se conoce como algoritmo de Shor presentan algunos riesgos para la criptografía actual. Se cree que algunos algoritmos de cifrado son irrompibles, excepto por ataques de fuerza bruta. Aunque los ataques de fuerza bruta pueden ser difíciles para las computadoras clásicas, serían fáciles para las computadoras cuánticas haciéndolos susceptibles a tales ataques (National Institute of Standards and Technology (NIST)., 2016).

Por ejemplo, algoritmos de cifrado como RSA, que se basan en la dificultad de factorizar números grandes, podrían ser fácilmente comprometidos por computadoras cuánticas debido a la eficiencia del algoritmo de Shor en la factorización. Esta capacidad no solo socava la seguridad de datos cifrados actualmente, sino que también plantea desafíos para la protección de la información en el futuro (Shor, P. W., 1994).

Es poco probable que los piratas informáticos y los ciberdelincuentes puedan permitirse las computadoras cuánticas en el futuro previsible. Sin embargo, los estados nacionales tienen la capacidad de pagarlas y administrarlas.

Conclusiones

¿Podría la computación cuántica ayudar a construir una computadora irrompible que sea realmente resistente a los ataques en el Internet de las Cosas, a pesar de las vulnerabilidades humanas?

La computación cuántica ha generado una gran expectación debido a su potencial para resolver problemas complejos de manera exponencialmente más rápida que las computadoras clásicas. Sin embargo, esta misma capacidad también plantea desafíos en términos de seguridad informática. La criptografía cuántica ofrece una solución prometedora al proporcionar un método de comunicación seguro que

se basa en los principios de la física cuántica, aprovechando la intrínseca imprevisibilidad de las partículas subatómicas para garantizar la seguridad de la transmisión de datos. A medida que la computación cuántica avanza, se proyecta que la criptografía cuántica desempeñará un papel crucial en la protección de información sensible en un mundo cada vez más interconectado y digitalizado. La capacidad de la criptografía cuántica para ofrecer métodos de cifrados resistentes a los ataques basados en algoritmos cuánticos representa un avance significativo en seguridad cibernética, especialmente en áreas críticas como el Internet de las Cosas (IoT), donde la salvaguarda de los datos es de máxima importancia.

Este es un tipo especial de clave de cifrado que es esencialmente irrompible. Pero existe cierta tranquilidad sobre el posible mal uso de la computación cuántica. Si bien cambiará la mayoría de los algoritmos de cifrado comúnmente utilizados en Internet, no es cierto que rompa todo el cifrado.

Los sistemas de cifrado que se utilizan para proteger los datos almacenados en registros y archivos de bases de datos utilizan una técnica diferente que la computación cuántica no ha podido romper hasta ahora.

Finalmente, es posible establecer que "Los sistemas ciberfísicos tienen consecuencias en el mundo real si se ven comprometidos. Incluso si un atacante no puede obtener el control, si puede acceder a la información, puede aprender, por ejemplo, cuando el propietario está ausente y otros hábitos potencialmente comprometedores. En este caso, los sistemas ciberfísicos incluyen no solo equipos como cámaras o controles de puerta, sino también infraestructuras inteligentes. (Ugwuishiwu, Chikodili & Orji, Ugochukwu & Ugwu, Celestine & Asogwa, Caroline., 2021).

Reconocimientos

Agradezco sinceramente a los centros de formación superior de la ciudad de Guayaquil como: Universidad Tecnológica Empresarial de Guayaquil, Universidad de Guayaquil, Espol, Universidad Bolivariana del Ecuador. Al equipo docente de la Revista Tecnológica - ESPOL RTE por su invaluable orientación y apoyo durante la elaboración de este trabajo investigativo: *"Las Vulnerabilidades de los Protocolos utilizados en el Internet de las Cosas (IoT)"*.

Agradezco profundamente a mis mentores y supervisores por su orientación y apoyo incondicional. Sus valiosas ideas y comentarios han sido fundamentales para la formulación y desarrollo de este trabajo.

Extiendo mi gratitud a los colegas e investigadores del campo de la ciberseguridad y la Internet de las cosas (IoT) por sus contribuciones

intelectuales y debates enriquecedores. Sus investigaciones previas y publicaciones han sido una fuente de inspiración y conocimiento.

Quisiera agradecer también a los participantes de los estudios experimentales y a los profesionales de la industria que compartieron su experiencia y perspectivas. Su colaboración ha sido esencial para la realización de los análisis y la obtención de resultados relevantes.

Finalmente, agradezco a mi familia, mi esposa, hijos y amigos por su constante apoyo y comprensión durante todo el proceso de esta investigación científica, su paciencia y ánimo han sido una fuente de fortaleza invaluable.

Referencias

Ahmed, P. (2020). *End to end for IoTnetworks.* Cryptography andSecurity 14(5), 345-360.

Arute, F., Arya, K., Babbush, R., Bacon, D., Bardin, J. C., Barends, R., ... & Martinis, J. M. (2019). La supremacía cuántica usando un procesador superconductor programable. Quantum supremacy using a programmable superconducting processor. Nature, 574(7779), 505-510: https://doi.org/10.1038/s41586-019-1666-5

Ashton, K. . (2009). *"That 'Internet of Things' Thing."* . RFID Journal.

Banerjee, S., & Kumar, D. (2021). *Advanced persistent threats in IoT systems.* ACM Transactions on Internet Technology, 20*(4), Article 28.

Quantum cryptography: Public key distribution and coin tossing. In Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Vol. 175, pp. 8-12.

Bennett, C. H., Brassard, G., & Ekert, A. K. (1992). *Quantum Cryptography: Public Key Distribution and Coin Tossing.* Proceedings of IEEE International Conference on Computers, Communications and Signal Processing.

Bertino, E. &. (2005). *Database Security – Concepts, Approaches, and Challenges.* IEEE Computer Society Press.

Brown, D. (2021). *Legal and regulatory aspects of IoT security.* Journal of Cyber Law, 15*(3), 45-60.

Brown, D. (2021). Legal and regulatory aspects of IoT security. Journal of Cyber Law, 15*(3), 45-60.

Chen, L., et al. (2022). *Post-Quantum Cryptography: An Overview.* IEEE Transactions on Information Forensics and Security.

CRYSTALS-Kyber Official Documentation. (2024). *CRYSTALS-Kyber Official Documentation.* CRYSTALS-Kyber Overview.

Davis, B., & Miller, E. (2020). *IoT device authentication mechanisms.* IEEE Internet of Things Magazine, 2*(1), 35-42.

Fernandez, L., & James, T. (2022). *Privacy-preserving techniques in IoT applications.* IEEE Transactions on Emerging Topics in Computing, 10(1), 180-192.

Gentry, C. &. (2017). *Fully Homomorphic Encryption without Bootstrapping from Standard Lattice Assumptions* . FOCS 2017.

Gisin, N., Ribordy, G., Tittel, W., & Zbinden, H. (2002). Quantum cryptography. Reviews of Modern Physics, . 74(1), 145-195.

Gomez, E., & Smith, R. (2021). *Security solutions for IoT healthcare systems.* Journal of Medical Internet Research, 23*(7), Article e2459.

Gupta, V. . (2022). *IoT security protocols: An overview.* International Journal of Security and Networks, 15*(1), 22-36.

Hewage, Asiri & Kamburugamuwa, Pasan. (2020). Quantum Cryptography for Internet of Things Security : A Review.

Ivanov, M., & Petrov, S. (2021). *Blockchain-based access control for IoT devices.* . International Journal of Distributed Ledger Technologies, 5*(4), 203-215.

Khan, A. (2020). *Best practices for device manufacturers.* . IEEE Consumer Electronics Magazine, 9*(2), 28-34.

Kumar, P. &. (2017). *Cryptographic Algorithms for IoT Security* . In Advances in Computer Communication and Computational Sciences. Springer.

Liu, C., & Wang, J. (2021). *Intrusion detection systems for IoT: Techniques and challenges.* Sensors, 21*(5), 1345-1360.

Marcos Allende López . (2019, Mayo 31). *Como funciona la computacion cuantica*. https://blogs.iadb.org/: https://blogs.iadb.org/conocimiento-abierto/es/como-funciona-lacomputacion-cuantica/

Martinez, H., & White, N. (2021). *Integrating IoT Devices with Cloud Security Solutions.* Journal of Cloud Computing, vol. 9, no. 2, pp. 210-225, 2021.

Melodie Roschman. (2024, Febrero 6). *https://uwaterloo.ca/*. https://uwaterloo.ca/news/mathematics/university-waterloo-joins-post-quantum-cryptography-alliance

Miguel Martínez R. (2015, 06/ 17). *https://www.telefonicaempresas.es/*. https://www.telefonicaempresas.es/grandes-empresas/blog/seguridad-y-privacidad-en-iot-estamos-a-tiempo/

Ministerio del Interior. (2015). *Secretaría de Estado de Seguridad. (n.d.). Gestión de Fondos Europeos.* Madrid-España: Retrieved from Ministerio del Interior.

Mosca, M. (2018). *The case for quantum-safe cryptography. Nature.* Ontario, Canada: 549(7671), 188-190.

National Institute of Standards and Technology . (2024). *Post-Quantum Cryptography (NIST).* NIST PQC.

National Institute of Standards and Technology (NIST). (2016). *Report on Post-Quantum Cryptography.* California: EEUU. NIST: https://www.nist.gov/

Nielsen, M. A., & Chuang, I. L. (2010). *Quantum Computation and Quantum Information.* Cambridge University Press.

Patel, N. &. (2020). *IoT security standards: A comprehensive review.* Computer Standards & Interfaces, 71*, 103-117.

Regev, O. (2009). *On Lattices, Learning with Errors, Random Linear Codes, and Cryptography* . Journal of the ACM.

Scarani, V., Bechmann-Pasquinucci, H., Cerf, N. J., Dušek, M., Lütkenhaus, N., & Peev, M. ((2009). The security of practical quantum key distribution. . *Reviews of Modern Physics,* , 81(3), 1301-1350.

Schneier, B. (2015). *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World.* W.W. Norton & Company.

Shannon, C. E. (1949). Communication Theory of Secrecy Systems. . *Bell System Technical Journal*, 28(4), 656-715.

Shor, P. W. . (1997). *Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer.* SIAM Journal on Computing, 26(5), 1484-1509. . https://doi.org/https://doi.org/10.1137/S0097539795293172

Shor, P. W. (1994). *lgorithms for quantum computation: discrete logarithms and factoring," Proceedings 35th Annual Symposium on Foundations of Computer Science, pp. 124-134, doi: 10.1109/SFCS.1994.365700.* Santa Fe, NM, USA: IEEE. In Proceedings 35th Annual Symposium on Foundations of Computer Science (pp. 124-134). IEEE.

Stallings, W., & Kaufman, C. (2015). *Computer Security: Principles and Practice.* Pearson.

Tanenbaum, A. S. (2011). *Computer Networks.* Prentice Hall.

Taylor, R., & Parker, J. (2020). *IoT security: A multi-layered approach.* Security and Privacy, 3*(2), Article e136.

Ugwuishiwu, Chikodili & Orji, Ugochukwu & Ugwu, Celestine & Asogwa, Caroline. (2021). *An overview of Quantum Cryptography and Shor's Algorithm.* . International Journal of Advanced Trends in Computer Science and Engineering. 9. 7487 – 7495. 10.30534/ijatcse/.

Wang, G., & Yang, F. (2021). *Securing IoT data in transit and at rest.* Journal of Data and Information Security, 12*(3), 123-140.

Zhou, M., & Zhang, L. . (2021). *Security vulnerabilities in IoT frameworks: A case study*. IEEE Transactions on Industrial Informatics, 17*(3), 1890-1902.

Zhou, W., Jia, Y., Peng, A., Zhang, Y., & and Peng Liu, I. (2018). *https://ieeexplore.ieee.org/ielaam/6488907/8709863/8386824-aam.pdf*. The Effect of IoT New Features on Security and: http://www.ieee.org/publications standards/publications/rights/index.html

Christian Vera Estrada

Aplicación de Ciberseguridad cuántica en la seguridad de puertos de comunicación de la IoT
Application of Quantum Cybersecurity in the security of IoT communication ports

Revista Tecnológica ESPOL - RTE
vol. 36, no. 2, p. 135 - 157, 2024
Escuela Superior Politécnica del Litoral, Ecuador
rte@espol.edu.ec

ISSN: 0257-1749
ISSN-E: 1390-3659

DOI: https://doi.org/10.37815/rte.v36n2.1188