Tecnologías Emergentes para la Ciberseguridad de dispositivos IoT

Rosin Zaira[1][0009-0004-4802-6688], Pujalte Denise[0009-0000-6298-2490], Dir. a/c Bolatti Diego[0000-0002-8275-4476]
Universidad Tecnológica Nacional UTN, Regional Resistencia, Chaco

rosinzaira@gmail.com, pujalte64@gmail.com, dbolatti@gfe.frre.utn.edu.ar

Resumen. En este trabajo se analiza la integración de la computación cuántica y técnicas de inteligencia artificial (IA) para mejorar la seguridad en dispositivos de Internet de las Cosas (IoT). Se presentan las principales amenazas a la ciberseguridad de IoT y se comparan diferentes soluciones basadas en computación cuántica y técnicas de IA. Además, se exploran las vulnerabilidades de los sistemas clásicos ante un entorno post-cuántico y se discuten medidas de seguridad como la Distribución de Claves Cuánticas (QKD) y criptografía post-cuántica. Finalmente, se concluye que la computación cuántica y las técnicas de IA pueden proporcionar niveles de seguridad superiores, aunque también presentan desafíos tecnológicos y de implementación.

Palabras clave: IoT, computación cuántica, machine learning. deep learning, ciberseguridad, inteligencia artificial.

1 Introducción

El Internet de las Cosas (IoT) es una red de dispositivos físicos que intercambian datos a través de internet. Estos dispositivos, como electrodomésticos y sensores, crean un ecosistema interconectado. Aunque ha transformado varios sectores, el IoT plantea preocupaciones sobre seguridad y privacidad, ya que las medidas tradicionales no son suficientes para abordar sus desafíos únicos. [1].

En la sección 2 se identifican vulnerabilidades en los sistemas actuales frente a amenazas post-cuánticas y se proponen varias soluciones para abordar estos problemas. Además, se exploran diversos ataques cuánticos y se presentan contramedidas específicas para mitigarlos. En la sección 3 se revisan técnicas de inteligencia artificial (IA), como el aprendizaje profundo, el aprendizaje incremental y la IA explicativa (XAI), y su aplicación en la detección y prevención de ataques cibernéticos en IoT. Se destacan soluciones como sistemas de detección de intrusiones y el análisis del comportamiento de usuarios y dispositivos para mejorar la seguridad. En la sección 4 se resumen los hallazgos principales y se discute el potencial de la computación cuántica y la IA para fortalecer la seguridad en IoT.

Este trabajo se enmarca en el proyecto: “Desarrollar un Marco de controles de ciberseguridad para gestión y control de funcionamiento de redes IoT.” de la UTN FRRe, CInApTIC, con el objetivo de explorar tecnologías emergentes en ciberseguridad para IoT, centradas en la inteligencia artificial y la computación cuántica.

1.1 Amenazas que enfrenta la ciberseguridad [2]

- Infracciones Físicas: Acceso no autorizado a dispositivos IoT, como la introducción de memorias USB maliciosas.
- Violaciones de Cifrado: Interceptación y almacenamiento de datos de dispositivos IoT no cifrados para su explotación futura.
- Denegación de Servicio (DDoS): Un servicio se vuelve inaccesible debido a una avalancha de solicitudes.
- Compromiso del Firmware: Exposición de dispositivos IoT a violaciones de ciberseguridad por falta de actualización de firmware.
- Explotaciones de Botnets: Dispositivos IoT se usan como bots para propagar malware.
- Ataques Man-in-the-Middle (MiTM): Interceptación de comunicaciones entre dos sistemas, engañando al destinatario para recibir mensajes falsificados.
- Ransomware: Cifra archivos, haciéndolos inaccesibles hasta obtener una clave de descifrado del atacante.
- Ataques de Escucha: Interceptación del tráfico de red para obtener información confidencial entre un dispositivo IoT y un servidor.

2 Computación cuántica

La aparición de algoritmos cuánticos tan potentes genera preocupación sobre la seguridad de las infraestructuras de IoT actuales. Si bien el cronograma para la disponibilidad de computadoras cuánticas a gran escala sigue siendo incierto, algunos expertos sostienen que los avances recientes sugieren su llegada dentro de unos pocos años, lo que hace que nuestros sistemas de IoT existentes sean vulnerables.[3]. Esta tecnología emergente explora el poder computacional de un sistema y mejora su rendimiento en términos de procesamiento de datos.

2.1 Vulnerabilidades [3]

Cifrado débil (CD): Uso de claves criptográficas insuficientes.
Contraseñas débiles (CC): Contraseñas fáciles de adivinar o codificadas inseguramente.
Servicios de red innecesarios (SRI): Ejecución de servicios no esenciales que comprometen la seguridad.
Interfaces inseguras (IE): Fallos en la autenticación y cifrado en sitios web, APIs y dispositivos móviles.
Falta de refuerzo físico (FR): Protección insuficiente de dispositivos IoT contra accesos no autorizados.

2.2 Tipos de ataques

Se presentan diversos tipos de ataques a sistemas IoT agrupados por capas de la arquitectura de los sistemas basados en IoT. Capa física: Manipulación de nodos, Fuerza bruta cuántica, Inyección de malware (MPIA), Basados en técnicas HLL y QKD. Capa de red: Inserción cuántica (ataque de redirección HTML), Recuperación de clave cuántica, De intermediario cuántico, Saturación cuántica, Intensidad del oscilador local (LO), Calibración cuántica. Capa de percepción: Estados falsos, Malware, Interferencia, Desincronización

cuántica, DDoS. Capa de aplicación: A la seguridad de bitcoins, De daño con láser, A la seguridad de contenedores en la nube. [3].

2.3 Soluciones [3]

- Módulos de Plataforma Confiable (TPM) que son chips de seguridad instalados en un dispositivo IoT cerca de la CPU. Este chip se utiliza principalmente para operaciones criptográficas, como la creación y el almacenamiento de claves de seguridad.
- QKD y QKR: Técnica de distribución de claves cuánticas (QKD) y el reciclaje de claves cuánticas (QKR). La primera comparte claves seguras entre dos partes. Si un intruso intenta interceptar la clave, se detecta automáticamente. Mientras que la segunda permite reutilizar una clave de forma segura, sin generar una nueva, usando estados cuánticos simples.
- ASLR: técnica de aleatorización del Diseño del Espacio de Direcciones (ASLR).
- Algoritmos de cifrado Grain-128 y Grain-128a encargados de generar claves de seguridad.
- Sellos cuánticos que proporcionan una técnica de codificación óptica cuántica utilizada en el remitente y pruebas de no localidad en el receptor para asegurarse de que no haya inyección de señales maliciosas en la fibra óptica.
- Análisis de paquetes basado en el número de secuencia y el valor TTL.
- Cifrado de extremo a extremo.

2.4 Ventajas y desventajas

Ventajas [3]:

- Potencia de Cálculo: Los algoritmos cuánticos pueden factorizar grandes números y resolver problemas algorítmicos con gran eficiencia.
- Seguridad Cuántica: Los métodos mencionados en el documento ofrecen una seguridad teóricamente invulnerable a los métodos tradicionales.
- Mitigación de Nuevas Amenazas: La computación cuántica puede generar nuevas amenazas, pero también ofrece soluciones, creando una carrera armamentista en ciberseguridad.

Desventajas [1]:

- Implementación: La infraestructura para la computación cuántica aún está en desarrollo y requiere una inversión significativa.
- Especialización: La implementación efectiva de tecnologías cuánticas requiere conocimientos altamente especializados que aún no están ampliamente disponibles.

3 Técnicas de Inteligencia Artificial

Algunas de las técnicas que proporcionan una defensa robusta y adaptable contra amenazas digitales son [4]:

- XAI: Asegura la transparencia en las decisiones de IA.
- Blockchain: Analiza el comportamiento para detectar patrones maliciosos.
- Aprendizaje Incremental: Se adapta a nuevas amenazas y evoluciona con el tiempo.
- Machine Learning: Analiza grandes datos para identificar comportamientos maliciosos.
- Deep Learning: Utiliza redes neuronales para una detección más precisa.

3.1 Soluciones empleando IA [5]

Algunas soluciones de seguridad basadas en IA son:

- IDS: Detectan ataques en tiempo real mediante análisis de tráfico de red.
- IPS: Previenen ataques bloqueándolos proactivamente.
- Análisis de comportamiento de usuarios y dispositivos: Detectan actividades anómalas con algoritmos de ML.
- Análisis de contenido malicioso: Identifican malware y amenazas de seguridad en archivos.
- Plataformas de gestión de amenazas: Correlacionan datos y patrones para una visión integral de seguridad.
- Soluciones de autenticación: Usan biometría y ML para verificar identidades.
- Detección de fraude: Identifican patrones sospechosos en transacciones.
- Respuesta automática a incidentes: Automatizan respuestas y medidas correctivas ante incidentes.

3.2 Ventajas y desventajas [6]

Ventajas

- Mejora de la Precisión Predictiva: Algoritmos de aprendizaje automático (ML) y aprendizaje profundo (DL) aumentan la precisión en la identificación de amenazas cibernéticas.
- Identificación de Tipos Específicos de Ciberataques: La IA distingue entre tráfico benigno y malicioso, detectando tipos específicos de ciberataques y activando medidas defensivas.
- Aplicación Amplia: Las técnicas de IA se utilizan en grandes empresas, agencias policiales y redes personales, añadiendo una capa extra de seguridad.

Desventajas

- Consumo de Recursos Computacionales: El aprendizaje profundo y otras técnicas de IA requieren mucha capacidad computacional para entrenamiento y operación.
- Susceptibilidad a Falsos Positivos: Los métodos basados en IA pueden generar falsos positivos, lo que puede llevar a respuestas defensivas innecesarias.
- Necesidad de Conjuntos de Datos Grandes y Representativos: Entrenar modelos de IA efectivamente requiere grandes conjuntos de datos, lo que puede ser desafiante en términos de recopilación y gestión.

4 Conclusiones

La computación cuántica puede proporcionar una base sólida y casi invulnerable para la seguridad criptográfica y la transmisión de datos, mientras que la IA ofrece una defensa dinámica y adaptable que evoluciona con nuevas amenazas. Juntas, estas tecnologías prometen una solución robusta, pero su implementación requerirá importantes inversiones en infraestructura y desarrollo especializado. Con el avance de estas tecnologías, se espera que desempeñen un papel clave en la protección de sistemas IoT frente a amenazas emergentes.

4.1 Consideraciones para futuras investigaciones

El campo emergente del aprendizaje automático cuántico (QML) emplea la mecánica cuántica como mecanismo de defensa. Aunque parece haber resultados iniciales prometedores en este nuevo campo, todavía existen obstáculos en el desarrollo de estas herramientas cuánticas para que sean resistentes para aplicaciones prácticas en el mundo real. [7]

Referencias

1. Quantum-empowered federated learning and 6G wireless networks for IoT security: Concept, challenges and future directions, https://www.sciencedirect.com/science/article/pii/S0167739X24003236, último acceso 23/07/24.
2. Fortifying home IoT security: A framework for comprehensive examination of vulnerabilities and intrusion detection strategies for smart cities ,https://www.sciencedirect.com/science/article/pii/S1110866524000069, último acceso 26/07/24.
3. Securing IoT systems in a post-quantum environment: Vulnerabilities, attacks, and possible solutions, https://www.sciencedirect.com/science/article/pii/S254266052400074X#section-cited-by, último acceso 23/07/24.
4. Aracelly Fernanda Alvarez C.: Estado del arte de técnicas de inteligencia artificial que aporten en la ciberseguridad, (2024).
5. Ciberseguridad en el IoT: escenario actual, buenas prácticas y riesgos, https://www.ikusi.com/mx/blog/ciberseguridad-en-el-iot-2/, último acceso 23/07/24.
6. Advancing Network Security in Industrial IoT: A Deep Dive into AI-Enabled Intrusion Detection Systems ,https://www.sciencedirect.com/science/article/abs/pii/S1474034624003331, último acceso 27/07/24.
7. Enhancing Internet of Medical Things security with artificial intelligence: A comprehensive review, https://www.sciencedirect.com/science/article/pii/S0010482524001203, último acceso 27/07/24.