ISBN: 978-628-95207-8-1. ISSN: 2414-6390. Digital Object Identifier: 10.18687/LACCEI2024.1.1.1206

Cybersecurity for the Protection of IOT Devices in the Industrial Sector

Oliva Olazábal, Alex Aleberto[1], Llanos Ñope, Clariza Margarith[2], Alarcón Vasquez, Segundo Felipe[3], León-Velarde Cesar Gerardo[4]
[1,2,3,4]Universidad Tecnológica del Perú (UTP), Lima, Perú
[1,2,3,4] 0513665@utp.edu.pe, U18102112@utp.edu.pe, c23460@utp.edu.pe, c19593@utp.pe

Abstract - With every passing day, new forms of attacks on IoT devices appear in the industrial sector. This research aims to identify common vulnerabilities, develop protection strategies, and establish guidelines to mitigate risks of cyber attacks. The PICO and PRISMA method was used to evaluate the review. Based on the established inclusion and exclusion criteria, 30 free access articles were selected from the Scopus, IEEE database corresponding to a systematic review of the literature. The analyzed results identified multiple vulnerabilities in industrial IoT devices, such as authentication failures, lack of data encryption, and firmware vulnerabilities. Security solutions were implemented, including firmware updates, implementation of robust encryption protocols, and staff training in cybersecurity best practices. The conclusions were reached: Cybersecurity in industrial IoT devices is crucial to prevent possible cyberattacks that could affect the production and integrity of the systems. Implementing preventive and corrective measures is essential to protect industrial infrastructure against constantly evolving cyber threats. It is also important to highlight the need for continued collaboration between manufacturers, operators and cybersecurity experts to ensure effective protection of IoT devices in the industrial sector.

Keywords - IoT, Cyber, Security, Threats, IoT Devices, Vulnerabilities, Mitigation, Authenticationbstract

Digital Object Identifier: (only for full papers, inserted by LACCEI).
ISSN, ISBN: (to be inserted by LACCEI).
DO NOT REMOVE

Ciberseguridad para la Protección de Dispositivos IoT en el Sector Industrial

Oliva Olazábal, Alex Aleberto[1], Llanos Ñope, Clariza Margarith[2], Alarcón Vasquez, Segundo Felipe[3], León-Velarde Cesar Gerardo[4]
[1,2,3,4]Universidad Tecnológica del Perú (UTP), Lima, Perú
[1, 2. 3. 4] 0513665@utp.edu.pe, U18102112@utp.edu.pe, c23460@utp.edu.pe, c19593@utp.pe

Resumen - Cada día que pasa aparecen nuevas formas de ataques a dispositivos IoT en el sector industrial. Esta investigación tiene como objetivo identificar vulnerabilidades comunes, desarrollar estrategias de protección y establecer pautas para mitigar los riesgos de ciberataques. Para evaluar la revisión se utilizó el método PICO y PRISMA. Con base en los criterios de inclusión y exclusión establecidos, se seleccionaron 30 artículos de libre acceso de la base de datos Scopus, IEEE correspondientes a una revisión sistemática de la literatura. Los resultados analizados identificaron múltiples vulnerabilidades en dispositivos industriales de IoT, como fallas de autenticación, falta de cifrado de datos y vulnerabilidades de firmware. Se implementaron soluciones de seguridad, incluidas actualizaciones de firmware, implementación de protocolos de cifrado sólidos y capacitación del personal en mejores prácticas de ciberseguridad. Se llegó a las conclusiones: La ciberseguridad en los dispositivos IoT industriales es crucial para prevenir posibles ciberataques que puedan afectar la producción e integridad de los sistemas. Implementar medidas preventivas y correctivas es esencial para proteger la infraestructura industrial contra amenazas cibernéticas en constante evolución. También es importante destacar la necesidad de una colaboración continua entre fabricantes, operadores y expertos en ciberseguridad para garantizar una protección eficaz de los dispositivos IoT en el sector industrial.
Palabras clave: IoT, cibernética, seguridad, amenazas, dispositivos IoT, vulnerabilidades, mitigación, resumen de autenticación.

I. INTRODUCCIÓN

Durante los últimos 5 años, el IoT ha ido transformando la forma en que interactuamos con el mundo físico y cómo se gestionan los datos, proporcionando la infraestructura y los datos en tiempo real de una variedad de dispositivos y sensores que hacen posible la toma de decisiones y el control avanzado [1], [3] , [4]. Por otro lado, la cibernética se enfoca en el control de sistemas, las redes, los dispositivos, los datos contra amenazas, ataques y accesos no autorizados, proporcionando herramientas para detectar y mitigar riesgos de manera efectiva. Juntos, estos campos tienen un impacto significativo en una variedad de aplicaciones, desde la industria hasta la salud y la movilidad [2].

El IoT ha experimentado un rápido crecimiento y ha transformado la forma en que interactuamos con el mundo. Sin embargo, el rápido aumento de los dispositivos IoT, que incluyen desde sensores inteligentes hasta electrodomésticos, ha expuesto vulnerabilidades de seguridad preocupantes que requieren soluciones efectivas y eficientes [2], [3], [5]. Por esta razón, es importante el uso de la seguridad cibernética para garantizar que los dispositivos IoT sean estables y confiables sin comprometer la integridad de los sistemas ni la privacidad de los usuarios [5].

La seguridad cibernética es fundamental para garantizar que los dispositivos IoT sean seguros y confiables. La falta de seguridad cibernética adecuada en IoT puede dar lugar a consecuencias graves, tanto en términos de pérdida de datos como de daño a la infraestructura y la reputación de una organización [2]. Por lo tanto, es esencial mejorar la seguridad cibernética en el diseño, implementación y operación de sistemas y dispositivos IoT. La combinación de la teoría de la cibernética con la capacidad de recopilar y examinar datos en tiempo real proporcionada por el IoT tiene el potencial de impulsar avances significativos en una amplia gama de aplicaciones [4].

En la presente revisión, se pretende comprender las medidas de seguridad y analizar métodos para la mitigación de los ataques y amenazas hacia los dispositivos IoT. Por lo tanto, el objetivo de este documento es identificar los ataques cibernéticos que pueden afectar en estos dispositivos y obtener los resultados de los métodos más utilizados para la evaluación de algoritmos de detección de intrusiones en entornos de IoT en el sector industrial [10], [12], [13], [14], [16], [21], [34].

Por consiguiente, el documento sigue esta estructura: La sección 2, llamada Metodología, se presenta el método utilizado para realizar la Revisión Sistemática de Literatura (RSL), aquí se describen los detalles desde las preguntas de investigación propuestas hasta las operaciones abordadas a la elección del material discutido en el documento. La sección 3 resultados, se muestran y analizan los resultados obtenidos en las diversas investigaciones como: Resultados sobre los métodos aplicados y analizados en los estudios de los dispositivos IoT, posibles vulnerabilidades de seguridad asociadas con sistemas IoT, resultados sobre medidas de Ciberseguridad para la protección de dispositivos IoT, resultados obtenidos sobre tipo de ataques a la seguridad en dispositivos IoT industriales. En la Sección 4, Discusión, Se plantea destacar la importancia de abordar las amenazas específicas que enfrenta los dispositivos IoT en entornos industriales. Se muestra la utilización de tecnologías como PUF (Physical Unclonable Functions), Bot-Iot, HoneyPot, CyberSec Labs, Dinámica paquetes IP, CICFlowMeter y la

Digital Object Identifier: (only for full papers, inserted by LACCEI).
ISSN, ISBN: (to be inserted by LACCEI).
DO NOT REMOVE

Arquitectura DINA, fundamentales para mitigar los ataques. Estas tecnologías ofrecen garantizar la protección mediante claves criptográficas, implementación de técnicas como Honeypot, que atraen y estudian posibles ataques fortaleciendo la autenticación y detectando dispositivos falsificados, contribuyendo así a una cadena de suministro más segura. Finalmente, en la sección 5, Conclusiones, se concreta que en las investigaciones se encuentra valiosa información sobre estrategias efectivas para asegurar los riesgos en los dispositivos industriales IoT. Se logra mitigar ataques en un rango del 85% al 96% destacando la relevancia de protocolos como PUF, la arquitectura RINA, CyberSec Labs, HoneyPot y CICFlowMeter. Se recomienda investigar las vulnerabilidades específicas en dispositivos IoT industriales y promover la implementación de procesos de inscripción seguros y DIF programables para abordar problemas de seguridad, privacidad y rendimiento

II. METODOLOGÍA

A. *PICO*

Se empleó la metodología PICO para estructurar búsquedas de información eficientes y enfocadas, lo primero que se requiere es la pregunta de investigación bien planteada. Idealmente debemos identificar los cuatro componentes principales: problema o paciente (P), intervención a analizar (I), comparación (C), resultados (O), y el componente opcional: contexto (C), facilitando la identificación precisa de datos relevantes, optimizando así la investigación y promoviendo la toma de decisiones fundamentada [6].

La pregunta que se formuló aplicando la metodología mencionada, es la siguiente: ¿En qué medida afecta la seguridad cibernética en el uso de los dispositivos IoT?

Posteriormente, se realizó subdivisión de la pregunta de investigación en preguntas asociadas a los componentes PICO:

- RQ1: ¿Cuál es la importancia de los dispositivos IoT en la actualidad?
- RQ2: ¿Cuáles son los dispositivos más utilizados?
- RQ3: ¿Qué vulnerabilidades de seguridad podría llegar a tener un sistema IoT?
- RQ4: ¿Cómo proteger la ciberseguridad en dispositivos IoT?

Palabra clave:
Se identificaron palabras clave para cada componente de la pregunta PICO, con el objetivo de estructurar una ecuación de búsqueda para obtener una cantidad adecuada de artículos científicos relevantes.

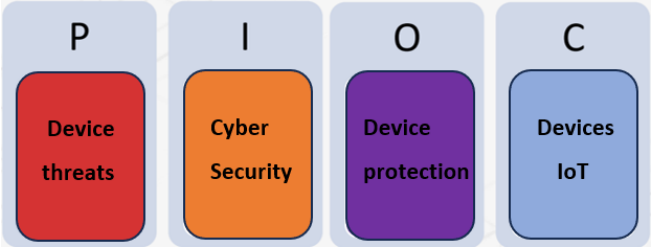

Figura 1: Cuadro PICO

Ecuación de búsqueda:
Se aplicó la ecuación de búsqueda sistemática en las bases de datos Scopus y IEEE:

("Threats" OR "attacks") AND ("IoT devices") AND ("Cyber security" OR "Device protection")

Cuadro PICO

En el siguiente cuadro se identificó los cuatro componentes principales:

Tabla 1: Método PICO

P	Amenazas de dispositivos.	“Threats” OR ”attacks” OR IoT devices
I	Seguridad cibernética.	“Cyber security” OR “Protection”
C		
O	Protección de dispositivos.	IoT devices OR Trusted devices
C	Dispositivos IoT	IoT devices

B. PRISMA

Se utilizó la metodología prisma para poder realizar una búsqueda más objetiva del RSL. La Declaración Prisma fue publicada en el año 2009 con la finalidad de ayudar a los investigadores a preparar un informe completo de su revisión sistemática e informar de manera transparente por qué se realizó la revisión, que métodos son empleados y qué artículos han encontrado los autores. [7].

Se tuvo en cuenta los siguientes criterios para analizar los artículos y detallar el diagrama Prisma, la cual se dividió en 3 partes: Identificación, Cribado e Incluidos.

Criterios de Inclusión:

CI 1 Se incluyó documentos tipo: Artículos de conferencia y Artículos científicos.

CI 2 Los estudios investigados contienen amenazas, ataques y accesos no autorizados a los dispositivos IoT.

CI 3 Se incluyó estudios de investigación respecto a la seguridad cibernética, de cómo detectar y mitigar riesgos de manera efectiva.

CI 4 Se incluyó publicaciones en idioma inglés.

Criterios de Exclusión:

CE 1 Se excluyó aquellos documentos que no cuentan con DOI.

CE 2 Se excluyó los artículos de investigación que no son de acceso libre.

CE 3 Se descartaron investigaciones de revistas.

CE 4 Se procedió a eliminar cualquier duplicado que surja durante la fase de búsqueda y selección de documentos.

En la fase de identificación se lograron identificar 710 artículos científicos. Después de analizar y hacer el proceso de detección se logró eliminar 78 artículos repetidos o duplicados; de esta manera, en la fase de cribado se obtuvieron hasta el momento 632 artículos. Posteriormente, al comparar el resumen y el título de los artículos seleccionados se excluyeron 515 artículos debido a que no se ajustaban al objetivo de investigación establecido, considerando los criterios de inclusión definidos; por ello, solo quedaron 117 publicaciones de artículos recuperadas para la evaluación. Continuando con el análisis se excluyó 1 publicación no recuperada, ya que era de paga y no de acceso libre. También, se realizó un filtro en las cuales 86 publicaciones fueron excluidas por las razones que se verán en el siguiente diagrama. Llegando a la fase de inclusión, se identificaron un total de 30 publicaciones que mostraban un potencial relevante y válido para la revisión.

De este modo, se detallan de manera gráfica y secuencial todos los procesos de búsqueda, identificación y selección de artículos relevantes para la investigación. Ver Fig. 2

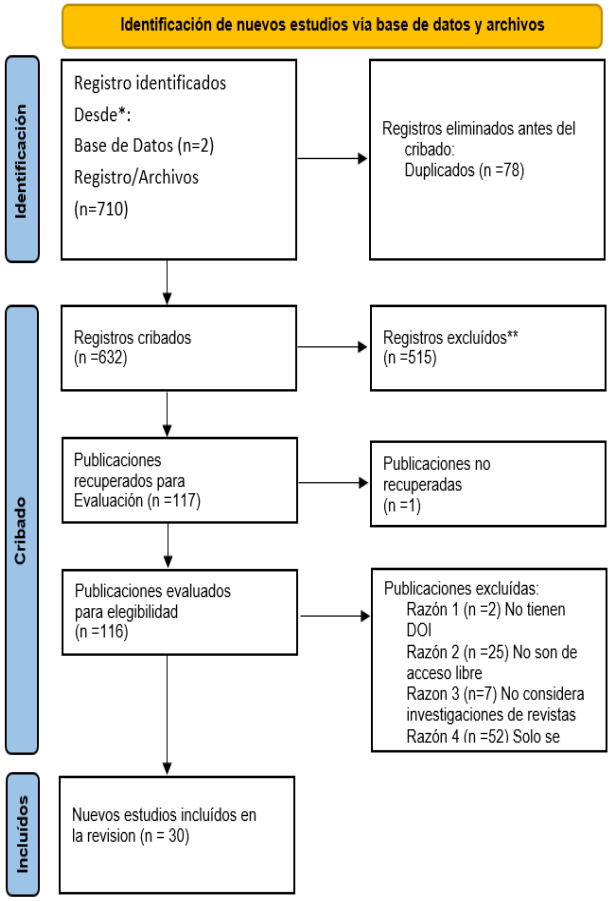

Figura 2: Diagrama de flujo PRISMA

III. RESULTADOS

3.1 Resultados de la cantidad de artículos sobre la ciberseguridad hacia los dispositivos IoT

Se escogieron 30 artículos de los últimos 5 años referentes a la investigación, los cuales buscan establecer un marco integral de seguridad cibernética que garantice la protección efectiva de los dispositivos IoT en la industria, asegurando la continuidad operativa y la integridad de los sistemas [8], [10]. Ver Fig. 3

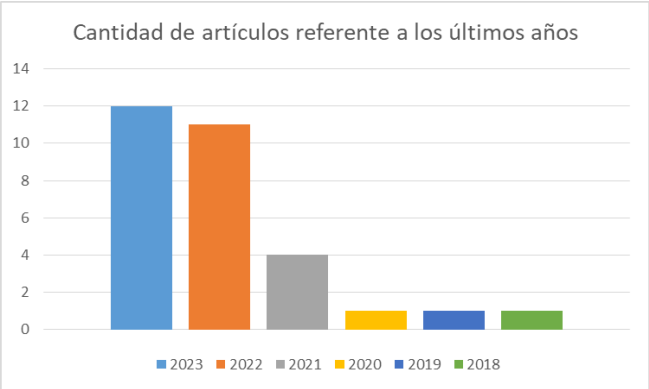

Figura 3: Cantidad de artículos de los últimos años

3.2 Resultados obtenidos de Países donde se realizaron las investigaciones de los artículos elegidos

En el siguiente gráfico se puede observar las investigaciones que utilizaron diferentes métodos para obtener el mejor resultado posible. Siendo Francia, el país que obtiene el mejor resultado, donde se aplica el método MUDL (Monitor, Understand, Defend, Adapt, Learn), el cual es un enfoque holístico para mitigar y responder a los ciberataques y se centra en cinco etapas clave: Monitorizar (Monitor), Comprender (Understand), Defender (Defend), Adaptar (Adapt), Aprender (Learn). Con la finalidad de mejorar aún más las capacidades de seguridad, reforzar la formación del personal y perfeccionar las estrategias de respuesta a incidentes [33], [34]. Ver Fig. 4

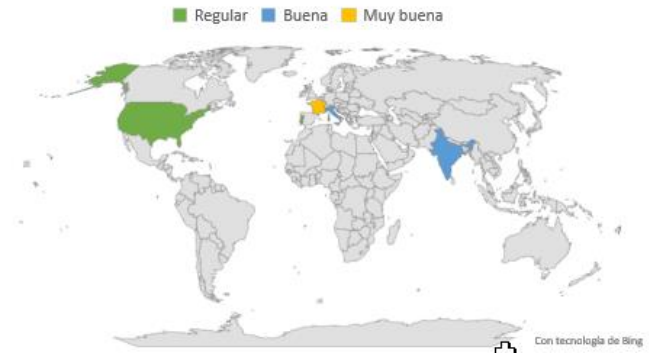

Figura 4: Países donde se realizaron métodos con resultados de medición para la mitigación de ataques y amenazas

3.3 Resultados de los dispositivos IoT más comunes en el sector industrial

Los dispositivos de IoT (Internet de las cosas) han experimentado un rápido crecimiento en los últimos años, y su diversidad ha aumentado significativamente [10], [12], [13], [14], [16], [19], [20], [29], [30]. En la siguiente tabla se puede observar los dispositivos de IoT más comunes en el sector industrial, clasificados por categoría. Ver Tabla 2.

Tabla 2: Dispositivos IoT en el sector Industrial

Categoría	Dispositivos IoT / descripción	Uso %
Sensores industriales	Sensores de temperatura, presión y humedad	10%
Sistemas de Monitización	Sistemas de monitoreo remoto de maquinaria y equipos	15%
Dispositivos de seguimiento	Disposicitovs de seguimiento de activos y productos	10%
Sistemas SCADA	Sistemas de control y Adquisición de Datos para supervisar y controlar procesos industriales	8%
Dispositivos de seguridad	Cámaras de vigilancia y sistemas de acceso biométrico	20%
Drones Industriales	Utilizados para inspecciones, mapeo y vigilancia	15%
Dispositivos de Mantenimiento Predictivo	Sensores para monitoreo del estado de la maquinaria Dispositivos para análisis predictivo de mantenimiento	10%
Sistemas de gestión de energía	Dispositivos para el monitoreo y control eficiente del consumo de energía en instalaciones industriales	12%

Estos dispositivos desempeñan un papel crucial en la transformación digital de las operaciones industriales, permitiendo la recopilación de datos en tiempo real, la mejora de la eficiencia y la toma de decisiones [12], [13], [16], [20], [30].

3.4 Resultados obtenidos sobre Tipo de Ataques a la seguridad en dispositivos IoT industriales

En el siguiente gráfico se proporcionó una visión general de los diferentes tipos de amenazas y ataques a la seguridad que pueden afectar a dispositivos IoT industriales. Es importante considerar estas amenazas al diseñar medidas de seguridad para proteger los sistemas industriales y garantizar su funcionamiento seguro y confiable [8], [10], [22], [28, [29], [32], [33]. Ver Fig. 5

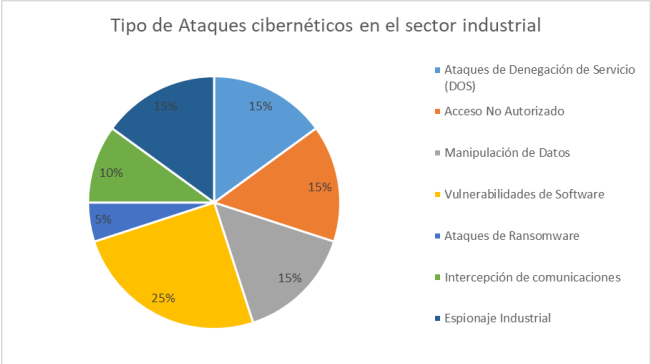

Figura 5: Gráfico sobre tipos de Ataques

Se puede observar que las vulnerabilidades de software en dispositivos IoT industriales son un punto crítico de preocupación, ya que podrían ser explotadas por actores malintencionados para comprometer la seguridad y la integridad de los sistemas industriales [33], [34].

3.5 Resultados sobre posibles vulnerabilidades de seguridad asociadas con sistemas IoT

Los sistemas IoT pueden ser susceptibles a diversas vulnerabilidades de seguridad debido a su complejidad, conectividad y la diversidad de dispositivos involucrados [33]. En el siguiente gráfico se puede observar que los problemas de autenticación tiene un punto crítico de 30%, siendo el mayor impacto negativo que podría llegar a tener un sistema IoT en el ámbito Industrial, debido a que los métodos de autenticación débiles o mal implementados pueden

permitir el acceso no autorizado a los dispositivos [22], [28], [15], [22], [33], [34]. Ver Fig. 6

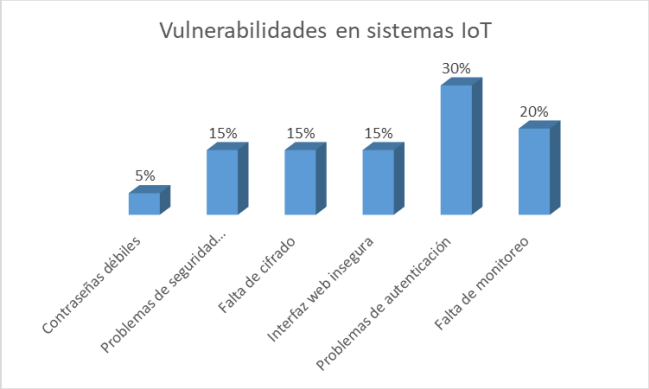

Figura 6: Gráfico sobre vulnerabilidades en sistemas IoT

3.6 Resultados sobre medidas de Ciberseguridad para la protección de dispositivos IoT

La seguridad en IoT es esencial para garantizar la confianza, proteger datos sensibles y mitigar una variedad de amenazas cibernéticas y físicas. La creciente adopción de dispositivos IoT destaca la importancia crítica de abordar los desafíos de seguridad asociados con esta tecnología en constante evolución. Para ello, se realizó una tabla que muestra 13 medidas de seguridad, las cuales proporcionan un enfoque integral para proteger dispositivos IoT [8], [10], [14], [15], [16], [21], 34]. Ver Tabla 3

Tabla 3: Medidas de Ciberseguridad para la protección de dispositivos IoT

N°	Medidas de Prevención	Descripción
1	Actualizaciones y Parches	Mantener todos los dispositivos y sistemas IoT actualizados con los últimos parches y actualizaciones de seguridad.
2	Configuración Segura	Cambia las credenciales y utiliza contraseñas fuertes en los dispositivos.
3	Actualización de Firmware	Los dispositivos IoT tienen un mecanismo de actualización de firmware seguro y realiza actualizaciones de manera regular
4	Encriptación de Datos	Utiliza encriptación para proteger la comunicación entre dispositivos IoT y otros sistemas.
5	Gestión de Identidad y Acceso	Implementa sistemas robustos de gestión de identidad y acceso para asegurar que solo usuarios autorizados tengan acceso a los dispositivos y sistemas.
6	Monitoreo Continuo	Establece sistemas de monitoreo continuo para detectar actividades anómalas o posibles intrusiones en tiempo real.
7	Detección de Intrusos	Utiliza sistemas de detección de intrusos para identificar comportamientos sospechosos y tomar medidas preventivas.
8	Auditorías de Seguridad	Realiza auditorías de seguridad periódicas para evaluar y mejorar las medidas de seguridad en los dispositivos IoT
9	Educación y Concientización	Capacitación a todos los empleados y usuarios sobre las mejoras de prácticas de seguridad y concientizar sobre posibles amenazas
10	Implementación de Principios de Diseño Seguro	Incorpora desde el diseño principios de seguridad para minimizar las vulnerabilidades desde el inicio
11	Análisis de Riesgos	Realiza análisis de riesgos para identificar y abordar posibles amenazas y vulnerabilidades específicas en el entorno industrial.
12	Cumplimiento de Normativas	Cumple con las normativas y estándares de seguridad relevantes para el sector industrial
13	Colaboración con la Comunidad de Seguridad	Participa en la comunidad de seguridad para estar al tanto de las últimas amenazas y soluciones, y colabora con otros en la industria para compartir conocimientos y mejores prácticas.

3.7 Resultados sobre los métodos utilizados en el estudio

En la siguiente imagen se muestra de forma detallada los métodos de investigación efectivos que se usaron para la protección ante la detección de ciberataques en los dispositivos IoT: Bot-Iot, Las PUFs, HoneyPot, CyberSec Labs, Dinámica paquetes IP, CICFlowMeter y la Arquitectura DINA, todos ellos están relacionados con aspectos específicos de la ciberseguridad, redes y tecnologías emergentes, ofreciendo la posibilidad de excluir las posibles amenazas o poner al dispositivo en estado de prevención. [4], [5], [8], [10], [12], [17], [18], [23], [32], [33], [34]. Ver Fig. 7

Figura 7: Métodos para la mitigación de ataques y amenazas

3.8 Resultados sobre los métodos analizados en el estudio

En la siguiente tabla se pueden observar los métodos analizados y el porcentaje de mitigación de ataques y amenazas hacia los dispositivos IoT en el sector industrial. Se puede observar que hay 3 herramientas que destacan por encima de las demás en el ámbito de la ciberseguridad de dispositivos IoT. Primero, las PUFs proporcionan una identidad única y no clonable para cada dispositivo IoT. Estas funciones se basan en las variaciones únicas que se producen durante la fabricación del dispositivo, lo que hace que sea extremadamente difícil duplicar o clonar la PUF de un dispositivo en particular [8], [10], [13], [17]. Segundo, el HoneyPots puede proporcionar valiosa información para fortalecer las defensas de seguridad, identificar nuevas amenazas y entender mejor las tácticas utilizadas por los ciberdelincuentes [17], [32, [33, [37]. Por último, CyberSec Lab realiza pruebas de seguridad, evaluación de vulnerabilidades para luego analizar los incidentes de seguridad en dispositivos IoT para mejorar las estrategias de mitigación y respuesta [10], [16], [19], [21], [29]. Ver Fig. 8

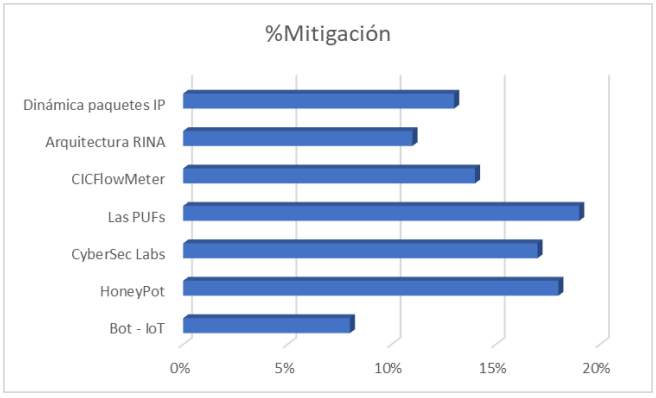

Figura 8: Métodos analizados para la mitigación de ataques y amenazas

IV. DISCUSIÓN

Se exploraron metodologías de investigación de vulnerabilidades, ataques, medidas, protocolos de autenticación, arquitecturas de comunicación segura, prevención de suplantación de IP y la percepción de amenazas en dispositivos IoT [4], [8], [10], [12]. Esta amplia revisión establece un marco sólido para comprender la seguridad cibernética en el contexto industrial de IoT y abordar los desafíos únicos y las amenazas específicas asociadas con estos dispositivos, garantizando así un entorno de IoT más seguro y resistente [14], [15], [21].

Las investigaciones revelan que la PUF es una de las herramientas más destacadas para la mitigación de ataques y amenazas hacia los dispositivos IoT, ya que contribuyen en mejorar la seguridad mediante la identidad única y no clonable, la protección de claves criptográficas, autenticación fuerte, la resistencia de ataques de clonación y la detección de dispositivos falsificados [10], [12], [16], [21]. Además, pueden desempeñar un papel crucial en la seguridad de la cadena de suministro de dispositivos IoT. Al vincular la identidad única de la PUF con la información del fabricante, se puede rastrear y verificar la autenticidad de cada dispositivo a lo largo de su ciclo de vida [13], [17], [20].

Se analizaron los métodos más utilizados y con mayor relevancia en el estudio, por un lado, “CyberSec Lab” se centra en proporcionar un entorno de laboratorio para la práctica y desarrollo de habilidades en ciberseguridad, por otro lado, "Honeypot" es una técnica específica de seguridad que se utiliza para atraer y estudiar a posibles atacantes. Un CyberSec Lab podría contener implementaciones de honeypots como parte de sus recursos para la investigación y la práctica en el campo de la ciberseguridad [4], [5], [8], [10], [12], [21].

V. CONCLUSIONES

Los resultados de las investigaciones proporcionan información valiosa sobre enfoques efectivos para abordar la seguridad cibernética en dispositivos IoT. Los protocolos de autenticación basados en PUF, la arquitectura de RINA, CyberSec Labs, HoneyPot y CICFlowMeter ofrecen perspectivas prácticas y teóricas para mitigar riesgos, destacando soluciones concretas para la protección de dispositivos industriales conectados. Se logró mitigar ataques dentro de margen (>=85% and <=96%) garantizando la seguridad del uso de los dispositivos IoT.

La eficiencia y escalabilidad de RINA pueden contribuir a la seguridad al garantizar que los dispositivos IoT puedan manejar eficientemente sus operaciones y responder a eventos de seguridad sin degradación del rendimiento; así mismo, aborda cuestiones de privacidad mediante la separación clara de funciones y la implementación de políticas de seguridad específicas. Esto puede ser importante en entornos de IoT donde la privacidad de los datos es una preocupación crítica.

Se recomienda abordar las limitaciones identificadas, estableciendo estándares para las pruebas de debilidades, mejorando la modelización de amenazas y promoviendo una documentación técnica más detallada. Además, se sugiere investigar a fondo las vulnerabilidades específicas en dispositivos IoT en el sector industrial, considerando la diversidad de amenazas y tecnologías emergentes.

Se propone para futuras investigaciones. Implementar procesos de inscripción seguros, garantizar que los IPCP estén autenticados antes de unirse a un DIF y DIF programables para abordar problemas de seguridad, privacidad y rendimiento.

Referencias

[1] Asharf, J., Moustafa, N., Khurshid, H., Debie, E., Haider, W., & Wahab, A. (2020). A review of intrusion detection systems using machine and deep learning in internet of things: Challenges, solutions and future directions. In Electronics (Switzerland) (Vol. 9, Issue 7). MDPI AG. https://doi.org/10.3390/electronics9071177

[2] Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions. In Electronics (Switzerland) (Vol. 12, Issue 6). MDPI. https://doi.org/10.3390/electronics12061333

[3] Haque, S., El-Moussa, F., Komninos, N., & Muttukrishnan, R. (2023). A Systematic Review of Data-Driven Attack Detection Trends in IoT. In Sensors (Basel, Switzerland) (Vol. 23, Issue 16). NLM (Medline). https://doi.org/10.3390/s23167191

[4] Jullian, O., Otero, B., Rodriguez, E., Gutierrez, N., Antona, H., & Canal, R. (2023). Deep-Learning Based Detection for Cyber-Attacks in IoT Networks: A Distributed Attack Detection Framework. Journal of Network and Systems Management, 31(2). https://doi.org/10.1007/s10922-023-09722-7

[5] Larriva-Novo, X., Villagrá, V. A., Vega-Barbas, M., Rivera, D., & Sanz Rodrigo, M. (2021). An IoT-focused intrusion detection system approach based on preprocessing characterization for cybersecurity datasets. Sensors (Switzerland), 21(2), 1–15. https://doi.org/10.3390/s21020656

[6] Quispe, A. M., Hinojosa-Ticona, Y., Miranda, H. A., & Sedano, C. A. (2021). Scientific writing series: Systematic review. In Revista del Cuerpo Médico Hospital Nacional Almanzor Aguinaga Asenjo (Vol. 14, Issue 1, pp. 94–99). Medical Body of the Almanzor Aguinaga Asenjo National Hospital. https://doi.org/10.35434/rcmhnaaa.2021.141.906

[7] Rethlefsen, M. L., & Page, M. J. (2022). PRISMA 2020 and PRISMA-S: common questions on tracking records and the flow diagram. In Journal of the Medical Library Association (Vol. 110, Issue 2, pp. 253–257). Medical Library Association. https://doi.org/10.5195/jmla.2022.1449

[8] Abbas, S. G., Vaccari, I., Hussain, F., Zahid, S., Fayyaz, U. U., Shah, G. A., Bakhshi, T., & Cambiaso, E. (2021). Identifying and mitigating phishing attack threats in IoT use cases using a threat modelling approach. Sensors, 21(14). https://doi.org/10.3390/s21144816

[9] Aldahmani, A., Ouni, B., Lestable, T., & Debbah, M. (2023). Cyber-Security of Embedded IoTs in Smart Homes: Challenges, Requirements, Countermeasures, and Trends. IEEE Open Journal of Vehicular Technology, 4, 281–292. https://doi.org/10.1109/OJVT.2023.3234069

[10] Alrowais, F., Althahabi, S., Alotaibi, S. S., Mohamed, A., Hamza, M. A., & Marzouk, R. (2023). Automated Machine Learning Enabled Cybersecurity Threat Detection in Internet of Things Environment. Computer Systems Science and Engineering, 45(1), 687–700. https://doi.org/10.32604/csse.2023.030188

[11] Amodei, A., Capriglione, D., Ferrigno, L., Miele, G., Tomasso, G., & Cerro, G. (2023). A measurement method for intrusion

detection in cyber IoT data stealing attacks. Conference Record - IEEE Instrumentation and Measurement Technology Conference, 2023-May. https://doi.org/10.1109/I2MTC53148.2023.10175888

[12] Aouedi, O., Piamrat, K., Muller, G., & Singh, K. (2023). Federated Semisupervised Learning for Attack Detection in Industrial Internet of Things. IEEE Transactions on Industrial Informatics, 19(1), 286–295. https://doi.org/10.1109/TII.2022.3156642

[13] Babaei, A., Schiele, G., & Zohner, M. (2022). Reconfigurable Security Architecture (RESA) Based on PUF for FPGA-Based IoT Devices. Sensors, 22(15). https://doi.org/10.3390/s22155577

[14] Bravos, G., Cabrera, A. J., Correa, C., Danilovic, D., Evangeliou, N., Ezov, G., Gajica, Z., Jakovetic, D., Kallipolitis, L., Lukic, M., Mascolo, J., Masera, D., Mazo, R., Mezei, I., Miaoudakis, A., Milosevic, N., Oliff, W., Robin, J., Smyrlis, M., … Vukobratovic, D. (2022). Cybersecurity for Industrial Internet of Things: Architecture, Models and Lessons Learned. IEEE Access, 10, 124747–124765. https://doi.org/10.1109/ACCESS.2022.3225074

[15] Diro, A. A., & Chilamkurti, N. (2018). Distributed attack detection scheme using deep learning approach for Internet of Things. Future Generation Computer Systems, 82, 761–768. https://doi.org/10.1016/j.future.2017.08.043

[16] Færøy, F. L., Yamin, M. M., Shukla, A., & Katt, B. (2023). Automatic Verification and Execution of Cyber Attack on IoT Devices. Sensors, 23(2). https://doi.org/10.3390/s23020733

[17] Gao, H., Li, L., Chang, X., Wan, J., Li, J., Du, J., & Zhang, X. (2022). BlockchainBot: A Novel Botnet Infrastructure Enhanced by Blockchain Technology and IoT. Electronics (Switzerland), 11(7). https://doi.org/10.3390/electronics11071065

[18] Khadidos, A. O., AlKubaisy, Z. M., Khadidos, A. O., Alyoubi, K. H., Alshareef, A. M., & Ragab, M. (2023). Binary Hunter–Prey Optimization with Machine Learning—Based Cybersecurity Solution on Internet of Things Environment. Sensors, 23(16). https://doi.org/10.3390/s23167207

[19] Kose, Y., Ozer, M., Bastug, M., Varlioglu, S., Basibuyuk, O., & Ponnakanti, H. P. (2021). Developing Cybersecurity Workforce: Introducing CyberSec Labs for Industry Standard Cybersecurity Training. Proceedings - 2021 International Conference on Computational Science and Computational Intelligence, CSCI 2021, 716–721. https://doi.org/10.1109/CSCI54926.2021.00184

[20] Lade, P., Ghosh, R., Bosch, R., & Srinivasan, S. (2017). Manufacturing Analytics and Industrial Internet of Things. www.computer.org/intelligent

[21] Latif, S., Huma, Z. E., Jamal, S. S., Ahmed, F., Ahmad, J., Zahid, A., Dashtipour, K., Aftab, M. U., Ahmad, M., & Abbasi, Q. H. (2022). Intrusion Detection Framework for the Internet of Things Using a Dense Random Neural Network. IEEE Transactions on Industrial Informatics, 18(9), 6435–6444. https://doi.org/10.1109/TII.2021.3130248

[22] Lysenko, S., Bobrovnikova, K., Kharchenko, V., & Savenko, O. (2022). IoT Multi-Vector Cyberattack Detection Based on Machine Learning Algorithms: Traffic Features Analysis, Experiments, and Efficiency. Algorithms, 15(7). https://doi.org/10.3390/a15070239

[23] Pawlicka, A., Puchalski, D., Pawlicki, M., Kozik, R., & Choraś, M. (2023). How to secure the IoT-based surveillance systems in an ELEGANT way. 636–640. https://doi.org/10.1109/csr57506.2023.10224938

[24] PES Institute of Technology (Bangalore, I., IEEE Communications Society, IEEE Photonics Society. Bangalore Chapter, IEEE Robotics and Automation Society. Bangalore Chapter, & Institute of Electrical and Electronics Engineers. (n.d.). 2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI) : 19-22 Sept. 2018 .

[25] Protogerou, A., Kopsacheilis, E. V., Mpatziakas, A., Papachristou, K., Theodorou, T. I., Papadopoulos, S., Drosou, A., & Tzovaras, D. (2022). Time Series Network Data Enabling Distributed Intelligence. A Holistic IoT Security Platform Solution. Electronics (Switzerland), 11(4). https://doi.org/10.3390/electronics11040529

[26] Qin, Y., Liu, J., Zhao, S., Feng, D., & Feng, W. (2020). RIPTE: Runtime Integrity Protection Based on Trusted Execution for IoT Device. Security and Communication Networks, 2020. https://doi.org/10.1155/2020/8957641

[27] Roldán-Gómez, J., Boubeta-Puig, J., Carrillo-Mondéjar, J., Castelo Gómez, J. M., & del Rincón, J. M. (2023). An automatic complex event processing rules generation system for the recognition of real-time IoT attack patterns. Engineering Applications of Artificial Intelligence, 123. https://doi.org/10.1016/j.engappai.2023.106344

[28] Samyuel, N. B., & Shimray, B. A. (2021). Securing IoT device communication against network flow attacks with Recursive Internetworking Architecture (RINA). ICT Express, 7(1), 110–114. https://doi.org/10.1016/j.icte.2020.08.001

[29] Shahin, M., Chen, F. F., Bouzary, H., Hosseinzadeh, A., & Rashidifar, R. (2022). A novel fully convolutional neural network approach for detection and classification of attacks on industrial IoT devices in smart manufacturing systems. International Journal of Advanced Manufacturing Technology, 123(5–6), 2017–2029. https://doi.org/10.1007/s00170-022-10259-3

[30] Shahin, M., Chen, F. F., Hosseinzadeh, A., Bouzary, H., & Rashidifar, R. (2022). A deep hybrid learning model for detection of cyber attacks in industrial IoT devices. International Journal of Advanced Manufacturing Technology, 123(5–6), 1973–1983. https://doi.org/10.1007/s00170-022-10329-6

[31] Shalaginov, A., & Azad, M. A. (2021). Securing resource-constrained iot nodes: Towards intelligent microcontroller-based attack detection in distributed smart applications. Future Internet, 13(11). https://doi.org/10.3390/fi13110272

[32] Sharma, P., Kapoor, S., & Sharma, R. (2023). Ransomware detection, prevention and protection in IoT devices using ML techniques based on dynamic analysis approach. International Journal of System Assurance Engineering and Management, 14(1), 287–296. https://doi.org/10.1007/s13198-022-01793-0

[33] Shokeen, R., Shanmugam, B., Kannoorpatti, K., Azam, S., Jonkman, M., & Alazab, M. (2019). Vulnerabilities analysis and security assessment framework for the internet of things. Proceedings - 2019 Cybersecurity and Cyberforensics Conference, CCC 2019, 22–29. https://doi.org/10.1109/CCC.2019.00-14

[34] Singh, A., & Sikdar, B. (2022). Adversarial Attack and Defence Strategies for Deep-Learning-Based IoT Device Classification Techniques. IEEE Internet of Things Journal, 9(4), 2602–2613. https://doi.org/10.1109/JIOT.2021.3138541

[35] Süren, E., Heiding, F., Olegård, J., & Lagerström, R. (2023). PatrIoT: practical and agile threat research for IoT. International Journal of Information Security, 22(1), 213–233. https://doi.org/10.1007/s10207-022-00633-3

[36] Udayakumar, R., Anuradha, M., Gajmal, Y. M., & Elankavi, R. (2023). Anomaly Detection for Internet of Things Security Attacks Based on Recent Optimal Federated Deep Learning Model. Journal of Internet Services and Information Security, 13(3), 104–121. https://doi.org/10.58346/JISIS.2023.I3.007

[37] Yerima, S. Y. (2023). High Accuracy Detection of Mobile Malware Using Machine Learning. In Electronics (Switzerland) (Vol. 12, Issue 6). MDPI. https://doi.org/10.3390/electronics12061408