Análisis de la ciberseguridad en protocolos de comunicación inalámbrica industrial[1]

Eduar Hernando Navas Valencia[2]
Oscar Fernando Becerra Angarita[3]

Resumen

Las comunicaciones inalámbricas industriales son fundamentales para la Industria 4.0 y el IIoT, pero su adopción incrementa los riesgos de ciberseguridad. Este trabajo presenta una revisión de los principales ataques que afectan la autenticación, integridad, confidencialidad y disponibilidad en redes industriales inalámbricas, así como de los mecanismos de mitigación más utilizados. Se analizan soluciones basadas en criptografía, autenticación, Intrusion Detection System/Intrusion Prevention System (IDS/IPS), blockchain, deep learning, anti-jamming, Software-Defined Networking (SDN) y modelos de confianza. Los resultados evidencian que la protección efectiva requiere una estrategia multicapa y que las técnicas de inteligencia artificial están adquiriendo un papel cada vez más relevante en la detección y mitigación de amenazas.

Palabras claves: Redes inalámbricas industriales, IIoT, SCADA, ciberseguridad, sistemas de detección de intrusiones.

Cybersecurity Analysis of Industrial Wireless Communication Protocols)

Abstract

Industrial wireless communications are a key enabling technology for Industry 4.0, IIoT, and cyber-physical systems, providing flexible and scalable connectivity for industrial devices and processes. However, their widespread adoption increases exposure to cybersecurity threats affecting authentication, integrity, confidentiality, and availability. This paper reviews the main attacks targeting industrial wireless networks and analyzes mitigation mechanisms reported in the literature, including cryptography, authentication schemes, IDS/IPS, blockchain, deep learning, anti-jamming techniques, SDN, and trust management models. The analysis shows that no single solution can address all threats, requiring a multilayer security approach. Furthermore, recent research highlights a growing integration of artificial intelligence and machine learning to enhance threat detection and adaptive defense capabilities in industrial environments.

Keywords: Industrial Wireless Networks, IIoT, SCADA, Cybersecurity, Intrusion Detection Systems.

---

[1] Artículo científico presentado como opción de grado para optar por el título de ingeniero mecatrónico.

[2] Autor de contacto: Eduar Hernando Navas Valencia. Estudiante de Ingeniería Mecatrónica de la Universidad Santo Tomas. Correo electrónico: Eduarhernando.navas@ustabuca.edu.co.

[3] Director: Oscar Fernando Becerra Angarita. Ingeniero Electrónico de la Universidad Pontificia Bolivariana. Magíster en Ingeniería Eléctrica de la Universidad Federal do Rio Grande do Sul. Docente de la facultad de ingeniería mecatrónica. Correo electrónico: oscar.becerra01@ustabuca.edu.co.

Introducción

La automatización industrial ha experimentado un crecimiento significativo debido a la incorporación de tecnologías digitales, redes de comunicación y sistemas interconectados asociados a la Industria 4.0. En este contexto, los protocolos de comunicación industrial desempeñan un papel fundamental al permitir el intercambio de información entre dispositivos, sensores, controladores y sistemas de supervisión dentro de los procesos industriales (Achaal et al, 2024), (Gan et al, 2025). Asimismo, la adopción del Internet Industrial de las Cosas (IIoT) ha ampliado las capacidades de monitoreo, control y automatización mediante la integración de una gran cantidad de dispositivos inteligentes conectados a través de redes industriales y plataformas de procesamiento de datos.

El aumento de la conectividad, la convergencia entre tecnologías de la información (IT) y tecnologías operacionales (OT), y la integración de redes industriales con infraestructuras IIoT han generado nuevos desafíos relacionados con la ciberseguridad. El diseño original de los protocolos industriales priorizo la eficiencia, la disponibilidad y los requisitos de tiempo real, dejando en segundo plano aspectos relacionados con la protección de la información y la seguridad de las comunicaciones. Esta situación ha provocado la aparición de vulnerabilidades que pueden ser aprovechadas mediante ataques cibernéticos como accesos no autorizados, interceptación de datos, denegación de servicio, manipulación de información y compromiso de dispositivos conectados (Singh Gaba et al, 2025).

La creciente incorporación de sensores inalámbricos, dispositivos IoT industriales, plataformas de edge computing y sistemas SCADA conectados incrementa la superficie de ataque y exige la implementación de mecanismos de protección cada vez más robustos.

Por esta razón, resulta necesario estudiar las características de los protocolos de comunicación industrial, así como las principales amenazas, vulnerabilidades y mecanismos de seguridad asociados a estos sistemas. Comprender cómo afectan los ataques a la confidencialidad, integridad, disponibilidad y autenticación de la información permite establecer estrategias adecuadas para reducir los riesgos en entornos industriales modernos.

La presente revisión bibliográfica tiene como propósito examinar la ciberseguridad en los protocolos de comunicación industrial y las redes IIoT, mediante la recopilación y evaluación de literatura científica y documentación especializada. Específicamente, se analizan vulnerabilidades y amenazas de las tecnologías inalámbricas, los ataques que afectan a los sistemas ciberfísicos, y las estrategias de mitigación propuestas para proteger las comunicaciones dentro del ecosistema de la Industria 4.0.

Metodología

La presente revisión bibliográfica se desarrolló mediante una revisión bibliográfica de literatura científica especializada, en las bases de datos IEEE Xplore, ScienceDirect y Web of Science. Plataformas seleccionadas debido a su amplia cobertura y relevancia en publicaciones indexadas sobre temas relacionados con la ingeniería y con especial énfasis en comunicaciones inalámbricas, redes industriales, automatización, Internet Industrial de las Cosas (IIoT) y ciberseguridad.

La búsqueda bibliográfica se realizó mediante ecuaciones de búsqueda construidas a partir de palabras clave relacionadas con comunicaciones industriales inalámbricas y ciberseguridad. Los principales términos utilizados fueron: "industrial wireless networks", "industrial communication", "IIoT security", "industrial cybersecurity", "SCADA security", "wireless industrial protocols" e "industrial network security". Estos términos se combinaron mediante operadores booleanos para conformar ecuaciones de búsqueda como:

("industrial wireless networks" OR "wireless industrial protocols") AND ("IIoT security" OR "industrial cybersecurity" OR "industrial network security")

Para la identificación de mecanismos de mitigación se emplearon ecuaciones específicas tales como:

("industrial wireless networks" OR IIoT) AND (cybersecurity OR security) AND (authentication OR encryption OR IDS OR IPS OR blockchain OR "deep learning" OR "anti-jamming" OR SDN OR "trust management")

Las ecuaciones fueron adaptadas según la sintaxis y los requisitos de cada base de datos consultada.

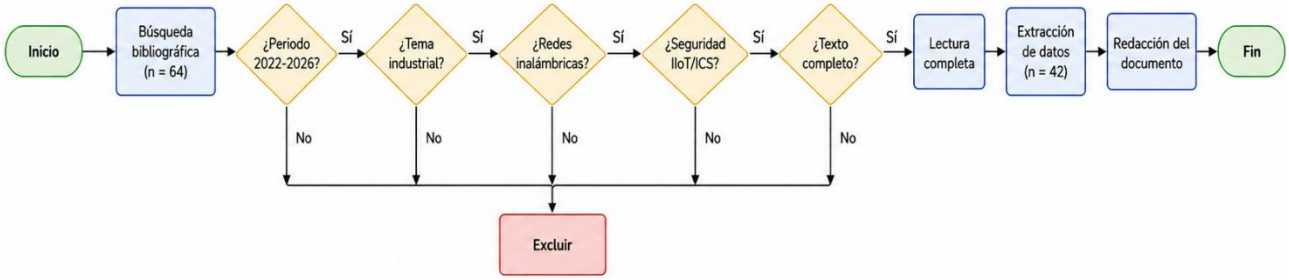
Tabla 1. *Conceptos de búsqueda y número de artículos revisados.*

Base de datos	Conceptos de búsqueda	Artículos encontrados	Artículos seleccionados
IEEE Xplore	Industrial IoT	4	3
IEEE Xplore	Industrial Wireless	8	3
IEEE Xplore	Industrial Wireless Security	15	11
IEEE Xplore	Industrial Wireless attack	26	20
ScienceDirect	Industrial Wireless Security and attack	6	3
Web of Science	Industrial Wireless Security and attack	5	2

Nota: *esta tabla presenta las principales cadenas de búsqueda utilizadas y el número de artículos recuperados y revisados en cada caso.*

El procedimiento general durante la revisión bibliográfica se presenta en la Figura 1.

Figura 1. *Diagrama De Flujo Del Proceso De Selección De Artículos.*

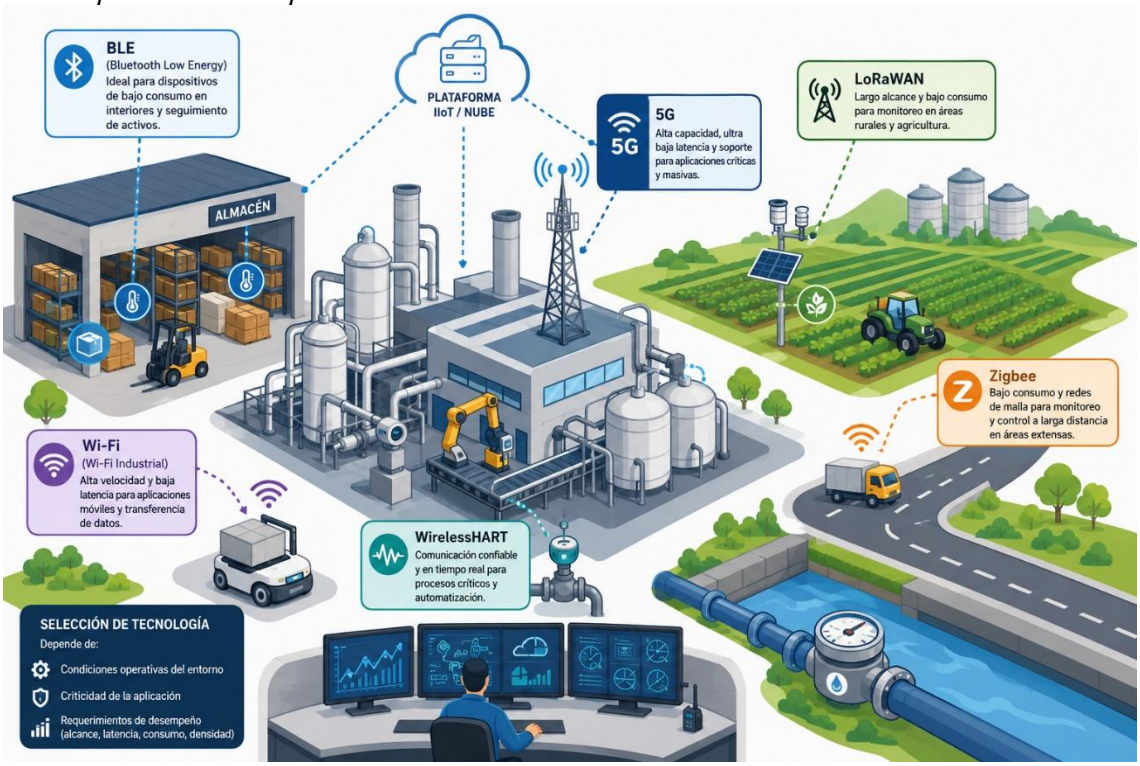


Protocolos inalámbricos industriales

Las comunicaciones industriales inalámbricas son uno de los pilares tecnológicos más importantes dentro de la Industria 4.0 y los sistemas ciberfísicos modernos. La evolución de los entornos industriales hacia arquitecturas inteligentes, altamente interconectadas y orientadas al Internet Industrial de las Cosas (IIoT) ha incremento la necesidad de mecanismos de comunicación flexibles, escalables y capaces de soportar grandes volúmenes de dispositivos distribuidos (Gaba et al, 2025). A diferencia de las redes cableadas tradicionales, las tecnologías inalámbricas permiten integrar sensores, actuadores, robots móviles, sistemas autónomos y plataformas de supervisión sin depender de infraestructura física compleja, facilitando la digitalización de procesos industriales, la movilidad operativa y la implementación de sistemas de monitoreo en tiempo real (Feng et al, 2025), (Drahoš et al, 2022). Este cambio tecnológico ha permitido el desarrollo de fábricas inteligentes capaces de intercambiar información continuamente entre equipos, plataformas de análisis y sistemas de control distribuidos.

El crecimiento de las redes inalámbricas industriales también ha sido impulsado por la necesidad de implementar arquitecturas más dinámicas y adaptables dentro de sectores como manufactura avanzada, minería, petróleo y gas, logística, agricultura inteligente y redes eléctricas inteligentes. Tecnologías como Wi-Fi industrial, Bluetooth Low Energy, Zigbee, WirelessHART, LoRaWAN, NB-IoT y 5G permiten cubrir diferentes requerimientos relacionados con alcance, latencia, consumo energético y densidad de dispositivos conectados (Gaba et al, 2025), (Marzieh Jalal Abadi et al, 2022), como se ve en la figura 2. Unas pocas tecnologías inalámbricas se orientan a aplicaciones de control y automatización, La gran mayoría se encarga del monitoreo distribuido, la adquisición periódica de datos o la conectividad masiva de sensores IoT de bajo consumo energético. Debido a esto, la selección de una tecnología inalámbrica industrial depende directamente de las condiciones operativas del entorno, lo critico de la aplicación y los requerimientos de desempeño de la red.

Figura 2. *Aplicaciones de protocolos inalámbricos de comunicación industrial*



Fuente: *Adaptado de (Drahoš et al., 2022) (Marzieh Jalal Abadi et al., 2022). Elaboración propia utilizando NotebookLM (2026).*

La incorporación masiva de comunicaciones inalámbricas dentro de infraestructuras industriales también introduce desafíos técnicos y de seguridad más complejos. El medio inalámbrico es inherentemente variable y susceptible a fenómenos como interferencia electromagnética, atenuación, desvanecimiento, multi trayectoria y congestión espectral, factores que afectan directamente la estabilidad y confiabilidad de la comunicación (Drahoš et al., 2022), (Marzieh Jalal Abadi et al, 2022). Estas limitaciones representan un reto importante para aplicaciones industriales críticas que requieren comportamiento determinista, baja latencia y alta disponibilidad, especialmente en sistemas de control en tiempo real y procesos sensibles a fallos de comunicación.

La unión entre tecnologías operacionales (OT), sistemas de información (IT), computación en la nube y dispositivos IIoT ha incrementado significativamente la superficie de ataque de las infraestructuras industriales modernas. Estudios recientes destacan que las redes industriales inalámbricas enfrentan amenazas relacionadas con interceptación de datos, ataques de denegación de servicio, manipulación de dispositivos, accesos no autorizados y explotación de vulnerabilidades en sistemas conectados (Achaal et al, 2024), (Singh Gaba et al, 2025). El incremento de dispositivos inteligentes y la interconexión masiva de sensores ha generado nuevos riesgos de privacidad y ciberseguridad que afectan directamente la disponibilidad, integridad y confidencialidad de la información industrial. Investigaciones recientes también demuestran que ataques avanzados pueden comprometer procesos físicos industriales mediante la explotación

coordinada de vulnerabilidades cibernéticas y sistemas automatizados, afectando incluso dispositivos robóticos y plataformas de manufactura inteligente (Gan et al, 2025).

Las tecnologías inalámbricas industriales modernas incorporan mecanismos avanzados de protección basados en autenticación, cifrado, gestión segura de identidades, segmentación de red y protocolos especializados de seguridad industrial. Sin embargo, la implementación efectiva de estos mecanismos es un desafío debido a las restricciones energéticas de muchos dispositivos IoT, la heterogeneidad tecnológica y la necesidad de mantener simultáneamente altos niveles de disponibilidad y desempeño en tiempo real. Por esta razón, organismos internacionales y estándares como IEC 62443 han adquirido un papel fundamental en el diseño seguro de infraestructuras industriales inalámbricas (Singh Gaba et al, 2025).

La norma IEC 62443 constituye uno de los marcos de referencia más utilizados para la ciberseguridad de sistemas de automatización y control industrial (IACS). Su objetivo es proporcionar un conjunto de requisitos, políticas y mecanismos de seguridad que permitan identificar riesgos, proteger activos críticos y aplicar estrategias de defensa en profundidad (Defense-in-Depth) a lo largo del ciclo de vida de los sistemas industriales, puede ver la estructura de la norma en la figura 3. La norma aborda aspectos relacionados con la gobernanza de la seguridad, el análisis de riesgos, el diseño de arquitecturas seguras y la implementación de controles de protección para dispositivos, redes y aplicaciones industriales (Schmittner et al, 2022).

Figura 3. *Estructura y ciclo de vida de la norma IEC 62443*

Fuente: *Adaptado de (Schmittner et al, 2022). Elaboración propia utilizando Notebooklm (2026).*

Clasificación de ataques en comunicaciones inalámbricas

Los sistemas IoT, Edge Computing e ICS/SCADA presentan múltiples vulnerabilidades debido a su arquitectura distribuida, la heterogeneidad de dispositivos y las limitaciones computacionales de muchos nodos conectados. Estas características incrementan la superficie de ataque y permiten que actores maliciosos comprometan principios fundamentales de seguridad como la disponibilidad, confidencialidad, integridad y autenticación. En entornos industriales, estas amenazas representan un riesgo crítico debido a que afectan procesos sensibles y sistemas de tiempo real.

a) Ataques de Autenticación

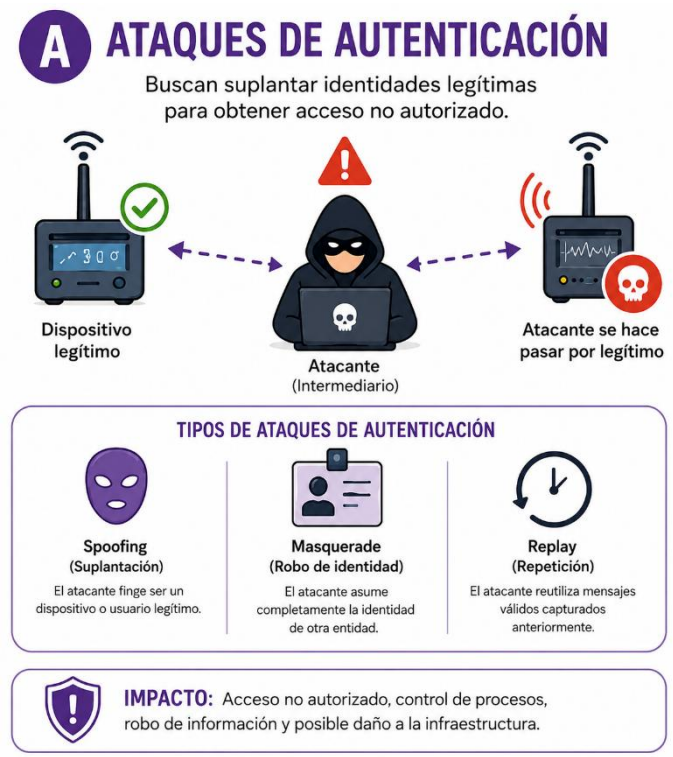
Los ataques de autenticación tienen como objetivo comprometer la verificación de identidad de los dispositivos, usuarios o nodos que participan en una red industrial inalámbrica. Este tipo de amenazas permite que un atacante suplante entidades legítimas dentro del sistema, obteniendo acceso no autorizado a información sensible o al control de procesos industriales. En entornos IoT, estos ataques representan un riesgo crítico debido a que los dispositivos intercambian constantemente datos relacionados con monitoreo, control y automatización (Al-Abadi et al., 2023).

Los ataques de spoofing, masquerade y replay buscan comprometer los mecanismos de autenticación de una red. En los ataques de spoofing, el atacante se hace pasar por un dispositivo confiable para enviar solicitudes falsas y acceder a información confidencial o alterar el funcionamiento del sistema. De manera similar, los ataques de masquerade permiten que un atacante robe identificadores de hardware o credenciales de dispositivos legítimos, logrando que la red lo reconozca como un nodo autorizado. Estas amenazas son especialmente peligrosas en aplicaciones industriales, ya que una orden falsificada puede modificar parámetros críticos de operación (Al-Abadi et al., 2023).

Ataque de repetición se basan en capturar comunicaciones legítimas y retransmitirlas posteriormente (Al-Abadi et al., 2023). Aunque los mensajes originales puedan estar cifrados, la reutilización de paquetes válidos puede provocar accesos indebidos, ejecución de acciones repetidas o alteraciones en la sincronización de los procesos. En sistemas industriales inalámbricos, donde existen limitaciones de recursos computacionales y latencias estrictas, estos ataques pueden pasar desapercibidos si no se implementan mecanismos robustos de autenticación y control temporal.

El ataque de fuerza bruta (Brute Force Attack) es una de las técnicas más utilizadas para comprometer sistemas de autenticación. Consiste en probar de manera sistemática múltiples combinaciones de nombres de usuario y contraseñas hasta encontrar las credenciales correctas y obtener acceso al sistema. El término "fuerza bruta" hace referencia al proceso de evaluar exhaustivamente todas las combinaciones posibles de claves o credenciales hasta identificar la válida (Sharma et al., 2024), como se ve en la figura 4.

Figura 4. *Esquema ataques de autenticación*



Fuente: adaptado de *(Al-Abadi et al., 2023). Elaboración propia utilizando Notebooklm (2026).*

En arquitecturas de edge computing e IoT industrial, las debilidades en autenticación se incrementan debido a la limitada capacidad de procesamiento de muchos dispositivos, la ausencia de interfaces de usuario y la falta de protocolos de seguridad estandarizados (Nirenjena et al., 2023). facilitando la propagación de botnets y la explotación de dispositivos vulnerables, permitiendo que atacantes obtengan control parcial o total sobre nodos industriales conectados.

b) Ataques de integridad

Los ataques de integridad buscan alterar, manipular o falsificar la información transmitida dentro de una red industrial inalámbrica. Su objetivo principal es comprometer la confiabilidad de los datos intercambiados entre sensores, controladores y sistemas de supervisión, provocando que las decisiones tomadas por el sistema se basen en información incorrecta o modificada. En aplicaciones industriales e IoT, la integridad de los datos es fundamental, ya que un atacante que modifique paquetes de información puede alterar variables críticas como temperatura, presión, velocidad o estados de actuadores, generando comportamientos inseguros o fallas operativas (Al-Abadi et al., 2023).

Un ejemplo son los ataques a la integridad de las medidas obtenida de sensores, donde el atacante manipula las mediciones de red mediante retrasos o pérdida intencional de paquetes para producir diagnósticos erróneos en los sistemas de monitoreo. Este tipo de ataque aprovecha la confianza implícita en las mediciones extremo a extremo utilizadas por técnicas de tomografía de

redes. En consecuencia, nodos legítimos pueden ser identificados incorrectamente como responsables de fallos o congestiones, convirtiéndose en un señuelo dentro de la red (Zhao et al., 2021).

Ataque Man-in-the-Middle (MITM) los atacantes interceptan la comunicación entre dos entidades legítimas y actúa como intermediario entre ambas, permitiendo capturar, modificar o falsificar la información transmitida sin que los participantes detecten la intrusión (Swain et al., 2022). El atacante puede manipular los mensajes intercambiados entre cliente y servidor, alterando datos críticos durante la transmisión y comprometiendo la confiabilidad del sistema. Esta capacidad de manipular datos en tránsito puede provocar errores en el monitoreo, diagnósticos incorrectos y decisiones operacionales erróneas dentro de infraestructuras críticas.

Ataque de inyección de paquetes (Packet Injection Attacks). Este tipo de ataque consiste en insertar paquetes maliciosos o manipulados dentro de la red de comunicación con el objetivo de alterar el comportamiento normal del sistema, comprometer la transmisión de datos o interrumpir los servicios de red (Dolai et al, 2025) como se ve en la figura 5. En entornos de comunicación industrial inalámbrica, estos ataques representan una amenaza crítica debido a la dependencia de la transmisión continua de información entre sensores, controladores y dispositivos de supervisión.

Figura 5. *Esquema de ataques de integridad.*

Fuente: adaptado de *(Al-Abadi et al, 2023) (Zhao et al, 2021). Elaboración propia utilizando Notebooklm (2026).*

Además, los atacantes pueden explotar nodos comprometidos para introducir retrasos artificiales o descartar paquetes específicos, afectando la percepción del estado real de la red (Zhao et al., 2021). Estas manipulaciones dificultan la detección de fallas reales y complican la implementación de mecanismos de recuperación o mitigación.

c) Ataques de confidencialidad

Los ataques de confidencialidad tienen como finalidad obtener acceso no autorizado a la información transmitida dentro de la red. En sistemas industriales inalámbricos, este tipo de ataque compromete la privacidad de los datos operacionales, credenciales de acceso, configuraciones de dispositivos y parámetros críticos de producción, como se muestra en la Figura 6.

La confidencialidad representa uno de los pilares fundamentales de la ciberseguridad en entornos IoT industriales y sistemas SCADA, debido a que la información intercambiada puede incluir datos sensibles relacionados con procesos de manufactura o supervisión remota. Cuando un atacante logra interceptar las comunicaciones, puede analizar el comportamiento del sistema y utilizar dicha información para preparar ataques más avanzados. Entre las amenazas más comunes se encuentran los ataques de análisis de tráfico, donde el atacante estudia el flujo de datos dentro de la red para identificar patrones de comunicación, ubicación de dispositivos y relaciones entre emisores y receptores. Aunque el contenido de los mensajes se encuentre cifrado, el análisis del comportamiento del tráfico puede revelar información sobre la infraestructura industrial y sus procesos operativos (Al-Abadi et al, 2023).

Debido a la naturaleza abierta del medio de comunicación, los protocolos inalámbricos industriales pueden ser vulnerables a técnicas de escucha pasiva (eavesdropping), especialmente cuando existen mecanismos débiles de cifrado o autenticación. Esto permite capturar paquetes, credenciales o configuraciones internas del sistema sin alterar directamente el funcionamiento de la red. (Kapicak et al, 2024)

El sniffing o captura de paquetes. Este ataque consiste en monitorear el tráfico de red y recopilar los paquetes de datos que circulan entre los dispositivos con el objetivo de obtener información sensible durante su transmisión. El sniffing puede clasificarse en dos modalidades principales: pasivo y activo. El sniffing pasivo se basa en la captura silenciosa del tráfico de red sin modificar los paquetes transmitidos, el sniffing activo implica la inserción o manipulación de tráfico dentro de la red para redirigir las comunicaciones hacia el atacante (Shaw et al., 2024).

Figura 6. *Esquema de ataques de confidencialidad.*

Fuente: adaptado de *(Kapicak et al., 2024) (Shaw et al., 2024). Elaboración propia utilizando Notebooklm (2026).*

En entornos edge computing, la confidencialidad también se ve afectada por la heterogeneidad de dispositivos y la falta de mecanismos de protección homogéneos (Baskaran et al., 2023). Muchos dispositivos IoT poseen recursos limitados y no implementan correctamente protocolos criptográficos robustos, aumentando la superficie de ataque y facilitando la filtración de información sensible. Adicionalmente, la gran cantidad de dispositivos conectados y la descentralización del procesamiento incrementan las dificultades para mantener políticas uniformes de protección de datos.

d) Ataques de disponibilidad

Los ataques de disponibilidad tienen como objetivo interrumpir o degradar el funcionamiento normal de la red, impidiendo que los servicios, dispositivos o aplicaciones industriales estén accesibles para los usuarios legítimos (Al-Abadi et al., 2023). En sistemas industriales inalámbricos y aplicaciones IoT, la disponibilidad es un requisito crítico debido a la necesidad de mantener comunicaciones continuas y tiempos de respuesta reducidos.

Los ataques de denegación de servicio (DoS) y denegación distribuida de servicio (DDoS) representan las amenazas más comunes dentro de esta categoría (Al-Abadi et al., 2023), (Baskaran et al., 2023). Estos ataques consisten en inundar servidores, dispositivos o redes con grandes cantidades de tráfico malicioso, agotando los recursos computacionales y de comunicación hasta provocar la interrupción parcial o total del servicio (Baskaran et al., 2023).

El jamming tiene como objetivo impedir o degradar las comunicaciones mediante la generación de interferencias en el canal de transmisión. Este ataque puede afectar directamente el funcionamiento de los protocolos de comunicación industrial inalámbricos al provocar pérdidas de paquetes, retrasos en la transmisión o incluso la interrupción total del enlace de comunicación. Entre las variantes más comunes se encuentran el constant jamming, en el que el atacante transmite señales de interferencia de forma continua ocupando el canal de comunicación, y el reactive jamming, donde la interferencia se genera únicamente cuando se detecta una transmisión legítima, optimizando así el uso de energía del atacante. Debido a que estos ataques comprometen la capacidad de los dispositivos para intercambiar información de manera confiable y oportuna, representan una amenaza significativa para la continuidad operativa y la estabilidad de los sistemas industriales inalámbricos (Pirayesh et al., 2022).

El flooding es un ataque dirigido contra la disponibilidad de la red, en el que un atacante genera y transmite una gran cantidad de solicitudes o paquetes con el propósito de agotar los recursos de los dispositivos de comunicación y provocar la degradación o interrupción del servicio. En el contexto de las redes industriales inalámbricas, este tipo de ataque puede saturar los nodos, puntos de acceso o dispositivos de encaminamiento, impidiendo que las solicitudes legítimas sean procesadas de manera oportuna. Una de sus variantes es el Interest Flooding Attack (IFA), donde el atacante envía un volumen masivo de solicitudes para mantener ocupados los recursos de la red y evitar la atención de peticiones legítimas. Además, versiones más sofisticadas incorporan nodos falsos o servidores controlados por el atacante para evadir los mecanismos de detección convencionales, aumentando así el impacto sobre el rendimiento y la disponibilidad de las comunicaciones (Jupriyadi et al., 2024).

En redes industriales y sistemas edge computing, los ataques DDoS son especialmente peligrosos debido a que muchos dispositivos poseen capacidades limitadas de procesamiento y mecanismos de defensa reducidos (Baskaran et al., 2023). Los atacantes suelen utilizar botnets compuestas por dispositivos IoT comprometidos para generar tráfico masivo hacia los servidores objetivo. Como consecuencia, los dispositivos legítimos no acceden a los recursos de red ni transmitir información crítica en tiempo real, ver figura 7.

Figura 7. *Esquema de ataques de disponibilidad.*

Fuente: adaptado de *(Baskaran et al., 2023)(Zeng, 2022). Elaboración propia utilizando Notebooklm (2026).*

Los ataques de retraso también afectan la disponibilidad de la información al provocar demoras en la entrega de mensajes prioritarios (Abdelhady et al., 2023). En aplicaciones industriales, donde existen restricciones temporales estrictas, un retraso excesivo puede impedir la ejecución correcta de acciones críticas o generar respuestas tardías ante situaciones de emergencia.

Las principales amenazas que afectan las comunicaciones industriales inalámbricas, la Figura 8 presenta la clasificación de los ataques de ciberseguridad según la propiedad de seguridad que buscan comprometer. Agrupando las amenazas en cuatro categorías principales: ataques de autenticación, orientados a la suplantación de identidad de dispositivos o usuarios; ataques de integridad, enfocados en la manipulación o alteración de la información transmitida; ataques de confidencialidad, dirigidos a la interceptación y obtención no autorizada de datos; y ataques de disponibilidad, cuyo objetivo es degradar o interrumpir el funcionamiento normal de la red. Esta clasificación permite identificar de manera estructurada los diferentes vectores de ataque presentes en entornos IoT industriales, Edge Computing y sistemas ICS/SCADA, así como comprender su impacto sobre los principios fundamentales de seguridad.

Figura 8. *Clasificación de los principales ataques en comunicaciones industriales.*

Fuente: adaptado de *(Abdelhady et al., 2023)(Jupriyadi et al, 2024). Elaboración propia utilizando Notebooklm (2026).*

Mecanismos de mitigación

a) Criptografía y Cifrado

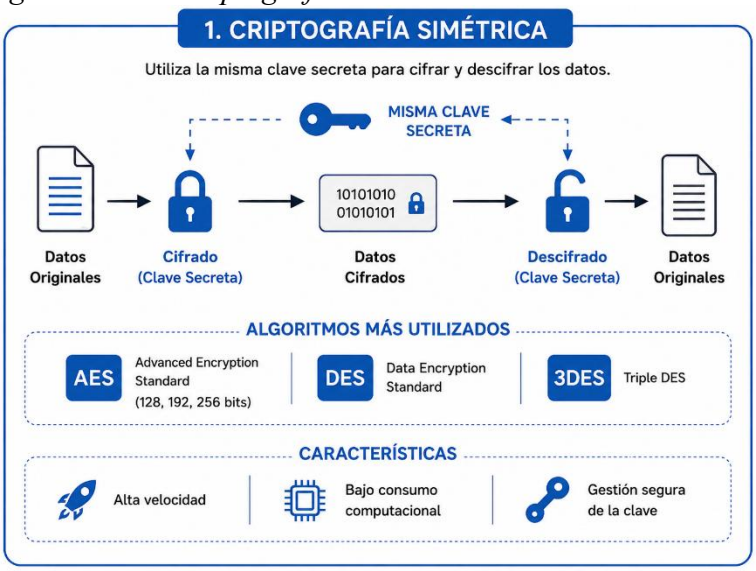
La criptografía es uno de los mecanismos de seguridad más utilizados para proteger la confidencialidad, integridad y autenticación de la información transmitida en redes industriales inalámbricas, sistemas IoT y arquitecturas de edge computing. Su objetivo es transformar los datos originales en información ilegible para usuarios no autorizados mediante el uso de algoritmos matemáticos y claves criptográficas. De esta manera, se garantiza que únicamente las entidades autorizadas puedan acceder o modificar la información intercambiada durante la comunicación (Kodela et al, 2025), (Wang et al, 2022).

Los mecanismos criptográficos protegen los datos frente a amenazas como la interceptación de comunicaciones, el acceso no autorizado, la manipulación de mensajes y los ataques dirigidos contra dispositivos industriales conectados. En entornos industriales, donde se intercambian continuamente datos de monitoreo, control y supervisión, la implementación de técnicas de cifrado permite asegurar la transmisión y almacenamiento de información sensible incluso en medios de comunicación potencialmente inseguros (Wang et al, 2022), ver la figura 9.

La criptografía utilizada en sistemas industriales puede clasificarse en criptografía simétrica y criptografía asimétrica. La criptografía simétrica usa una misma clave para los procesos de cifrado y descifrado, teniendo altas velocidades de procesamiento y bajo consumo computacional. Entre los algoritmos más utilizados se encuentra el Advanced Encryption Standard (AES), usado por su eficiencia y nivel de seguridad, con tamaños de clave de 128, 192 y 256 bits

(Kodela, 2025). Asimismo, otros algoritmos simétricos como DES y 3DES han sido utilizados históricamente en aplicaciones industriales, aunque actualmente presentan limitaciones frente a los requerimientos modernos de seguridad (Wang et al, 2022).

Figura 9. *Arquitectura general de la criptografía simétrica.*

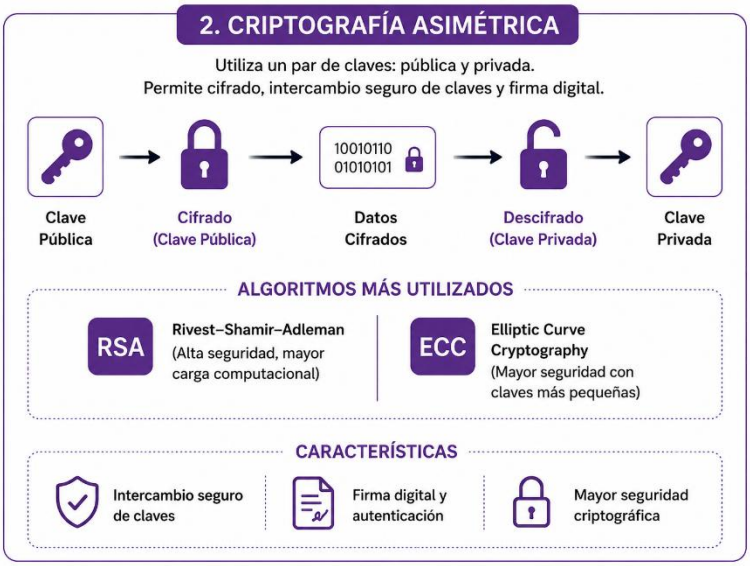


Fuente: adaptado de *(Kodela et al, 2025), (Wang et al, 2022).Elaboración propia utilizando Notebooklm (2026).*

Por otra parte, la criptografía asimétrica utiliza un par de claves, una pública y una privada, para realizar los procesos de cifrado, intercambio seguro de claves y firma digital. Entre los algoritmos más representativos se encuentran Rivest-Shamir-Adleman (RSA) y Elliptic Curve Cryptography (ECC). RSA teniendo altos niveles de seguridad para el intercambio de claves y autenticación digital, aunque consumiendo más recursos computacionales por a la complejidad de sus operaciones matemáticas (Kodela et al, 2025), (Wang et al, 2022). ECC proporciona niveles de seguridad utilizando claves más pequeñas, reduciendo el consumo de memoria, ancho de banda y recursos de procesamiento (Wang et al, 2022), ver la figura 10.

.

Figura 10. *Arquitectura general de la criptografía asimétrica.*



Fuente: adaptado de *(Kodela et al, 2025) (Wang et al, 2022). Elaboración propia utilizando Notebooklm*

Debido a las ventajas y limitaciones de cada una, las arquitecturas modernas de comunicaciones industriales emplean esquemas de cifrado híbrido que combinan algoritmos simétricos y asimétricos. En estos esquemas, algoritmos como AES son utilizados para cifrar grandes volúmenes de datos debido a su rapidez, mientras que algoritmos como RSA o ECC se emplean para el intercambio seguro de claves y la implementación de firmas digitales (Kodela et al, 2025), (Wang et al, 2022). Esta combinación aprovecha la eficiencia del cifrado simétrico junto con las capacidades de autenticación y distribución segura de claves proporcionadas por la criptografía asimétrica, ver la figura 11.

Figura 11. *Arquitectura general de la criptografía hibrida.*

Fuente: adaptado de *(Kodela et al, 2025), (Wang et al, 2022). Elaboración propia utilizando Notebooklm (2026).*

En aplicaciones de agricultura inteligente basadas en LoRaWAN, (Sokullu et al, 2022) desarrolló una red IoT para monitoreo de variables ambientales como temperatura, humedad, radiación UV e intensidad lumínica mediante nodos de bajo consumo energético. Aunque el sistema implementó mecanismos de autenticación mediante credenciales de usuario almacenadas en Google Firebase, los resultados evidenciaron la necesidad de incorporar cifrado de los datos transmitidos entre nodos y gateway para aumentar la confiabilidad de las comunicaciones. Los autores mencionan que el uso de mecanismos de cifrado permitiría establecer una comunicación más segura frente a ataques de interceptación o acceso no autorizado, especialmente en aplicaciones agrícolas desplegadas sobre grandes áreas geográficas donde la transmisión inalámbrica representa una superficie de ataque importante (Sokullu et al, 2022).

De manera similar, Haka et al. (Haka et al, 2025) abordaron la protección de redes ZigBee utilizadas en aplicaciones IoT mediante un esquema adaptativo de cifrado basado en AES. El trabajo propone que el Trust Center seleccione dinámicamente claves AES de 128, 192 o 256 bits de acuerdo con las capacidades criptográficas de cada dispositivo. Esto busca fortalecer el proceso de distribución de la Network Key (NWK), siendo uno de los elementos más críticos de la seguridad en ZigBee. Los resultados demostraron que los dispositivos configurados con AES-256 alcanzaron mayores niveles de seguridad, seguidos por AES-192 y AES-128, manteniendo la compatibilidad con la infraestructura existente. La propuesta permite mejorar la resistencia frente a ataques de interceptación de claves, análisis de tráfico y acceso no autorizado sin afectar la interoperabilidad de la red (Haka et al, 2025).

b) Autenticación

La autenticación mutua es un mecanismo de seguridad mediante el cual dos dispositivos verifican su identidad antes de intercambiar información o establecer una clave de sesión. Su objetivo es prevenir ataques de suplantación de identidad, dispositivos falsificados y accesos no autorizados (Gong et al, 2024).

En sistemas SCADA, se ha propuesto un esquema ligero de autenticación mutua basado en polinomios simétricos. Los dispositivos maestro y esclavo intercambian identificadores y calculan independientemente el valor de un polinomio compartido. Si ambos resultados coinciden, la autenticación se considera válida y el valor obtenido se utiliza para derivar una clave de sesión empleada posteriormente en el cifrado AES de las comunicaciones (Lu et al, 2016).

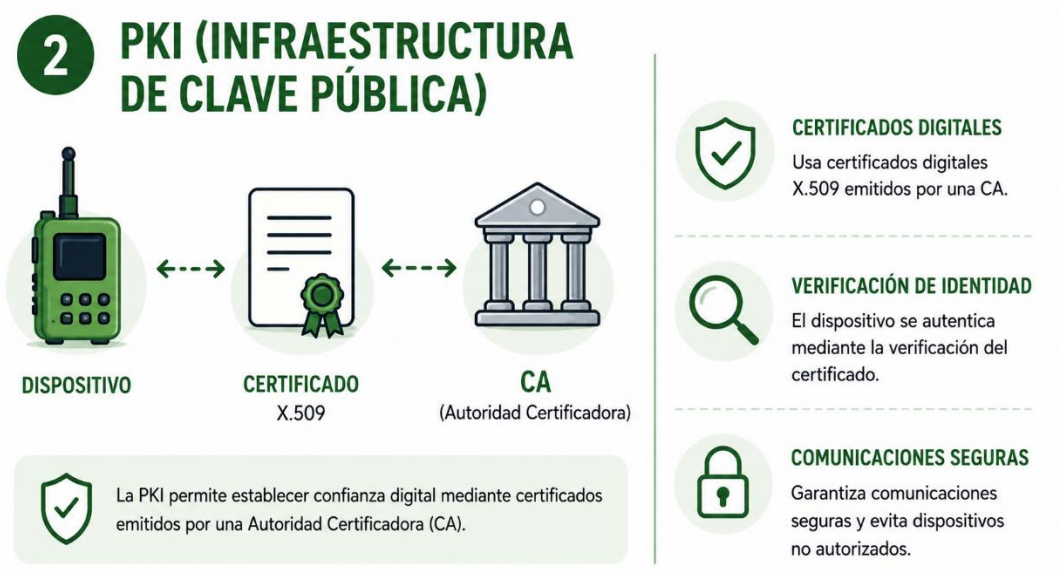
Para entornos IIoT, se ha desarrollado un esquema de autenticación mutua sin certificados (certificateless) basado en firmas digitales ligeras ver la figura 12. En este método, los dispositivos intercambian mensajes de autenticación que contienen parámetros criptográficos y firmas verificables, permitiendo confirmar la legitimidad de ambas partes y establecer una clave de sesión compartida. El protocolo fue diseñado para reducir el costo computacional y de comunicación en dispositivos con recursos limitados (Gong et al, 2024).

Figura 12. *Componentes asociados a la autenticación mutua.*

Fuente: adaptado de *(Gong et al, 2024). Elaboración propia utilizando Notebooklm (2026).*

La Infraestructura de Clave Pública (PKI) es un mecanismo ampliamente utilizado para la autenticación de dispositivos en entornos IoT e IIoT. Su funcionamiento se basa en certificados digitales X.509 emitidos por una Autoridad Certificadora (CA), los cuales vinculan la identidad de un dispositivo con una clave pública verificable. Durante el proceso de autenticación, los dispositivos intercambian certificados firmados criptográficamente cuya validez se comprueba mediante la clave pública de la CA, permitiendo establecer comunicaciones seguras y prevenir el acceso de dispositivos no autorizados a la red (Krishnan et al, 2022).

Figura 13. *Componentes asociados a la Infraestructura de Clave Pública (PKI).*



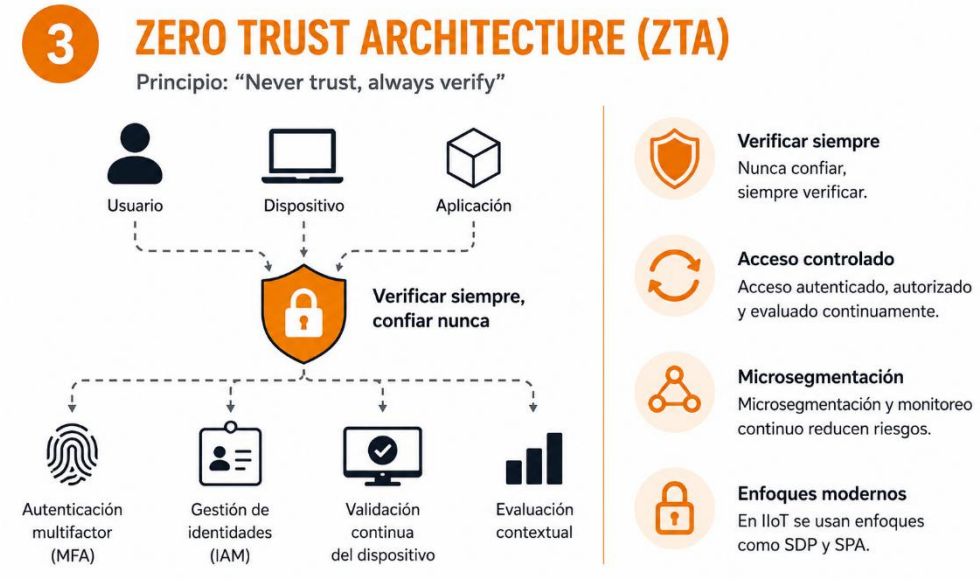
Fuente: adaptado de *(Krishnan et al, 2022). Elaboración propia utilizando Notebooklm (2026).*

Por otro lado tenemos una Arquitectura más robusta, como es Zero Trust (ZTA) es una alternativa a los modelos tradicionales de seguridad perimetral, basándose en el principio de "never trust, always verify" (Kumar et al, 2025). En este, ningún usuario, dispositivo o aplicación recibe confianza implícita, independientemente de su ubicación dentro o fuera de la red. Cada solicitud de acceso debe ser autenticada, autorizada y evaluada continuamente antes de permitir el acceso a los recursos (Kumar et al, 2025), (Singh et al, 2023).

En términos de autenticación, ZTA no depende de un código o credencial transmitida durante el acceso. En su lugar, emplea mecanismos como autenticación multifactor, gestión de identidades y accesos (IAM), validación continua de dispositivos y evaluación contextual basada en atributos como identidad, estado de seguridad del equipo, ubicación y nivel de riesgo detectado (Kumar et al, 2025), (Singh et al, 2023). Estas verificaciones son procesadas por componentes de decisión y aplicación de políticas que determinan dinámicamente si una solicitud debe ser permitida o rechazada (Kumar et al, 2025).

ZTA incorpora técnicas como microsegmentación, monitoreo continuo y análisis de comportamiento para reducir la superficie de ataque y limitar movimientos laterales dentro de la red (Kumar et al, 2025), ver la figura 14. En entornos IIoT, se han propuesto soluciones basadas en Software Defined Perimeter (SDP) y Single Packet Authorization (SPA), donde los dispositivos deben autenticar su identidad mediante credenciales criptográficas o firmas digitales antes de establecer una conexión con los servicios industriales, reforzando el control de acceso y reduciendo la dependencia de mecanismos tradicionales basados únicamente en contraseñas (Cheng et al, 2025).

Figura 14. *Componentes asociados a la Infraestructura de Clave Pública (PKI).*



Fuente: adaptado de *(Cheng et al, 2025). Elaboración propia utilizando Notebooklm (2026).*

La aplicación de mecanismos de autenticación en entornos IoT e IIoT ha demostrado mejoras en la protección de dispositivos y redes industriales. En redes LoRaWAN, se implementó un esquema ligero de autenticación basado en Zero Trust y blockchain tipo Proof-of-Authority,

complementado con autenticación mutua de bajo costo computacional. Los resultados mostraron una disponibilidad superior al 99.9 % y un retardo promedio de autenticación de 187 ms, manteniendo la viabilidad operativa en dispositivos de recursos limitados (Abdelhady et al, 2026).

En redes inalámbricas industriales de sensores (IWSN), se propuso un esquema de autenticación y acuerdo de claves (AKA) basado en Physical Unclonable Functions (PUF). El mecanismo utiliza el intercambio de mensajes de autenticación que contienen identificadores temporales, parámetros criptográficos y valores derivados de la PUF para verificar la identidad de los participantes y establecer una clave de sesión compartida. Las evaluaciones demostraron resistencia frente a ataques de intermediario (Man-in-the-Middle), repetición (replay) y ataques de modelado mediante aprendizaje automático, manteniendo bajos costos de comunicación y procesamiento (Yu et al, 2026).

En conjunto, los resultados reportados en diferentes entornos industriales muestran que los mecanismos modernos de autenticación no se limitan al uso de contraseñas o identificadores estáticos. Actualmente predominan esquemas basados en certificados digitales, firmas criptográficas, autenticación mutua, gestión dinámica de identidades y establecimiento seguro de claves de sesión, permitiendo reducir el riesgo de suplantación de dispositivos y accesos no autorizados en redes IIoT e industriales (Yin et al, 2024)–(Yu et al, 2026).

c) Sistemas IDS/IPS

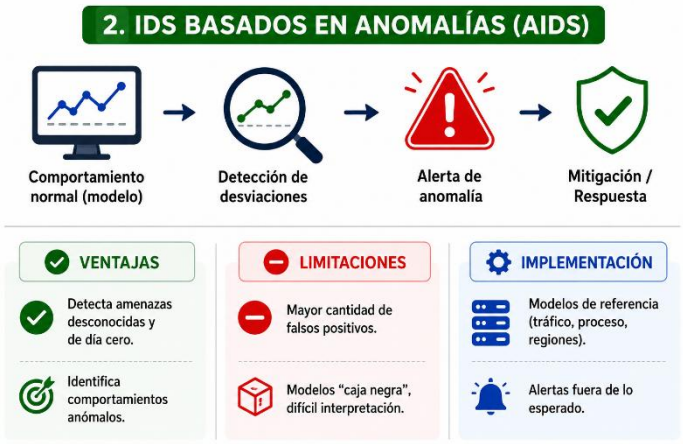
Los sistemas de detección de intrusiones basados en firmas (SIDS) son uno de los enfoques más utilizados para proteger redes industriales e IIoT. Su funcionamiento consiste en comparar el tráfico de red o los eventos del sistema con una base de datos de patrones conocidos de actividades maliciosas, generando alertas cuando se detectan coincidencias. Su principal ventaja es la alta precisión en la detección de ataques previamente documentados y sus bajas tasas de falsos positivos, pudiendo implementarse tanto en sistemas de detección de intrusiones de red (NIDS) como basados en host (HIDS), como se muestra en la Figura 15. Sin embargo, su eficacia depende de la actualización constante de las firmas, lo que limita su capacidad para identificar ataques de día cero, variantes modificadas de malware o amenazas previamente desconocidas (Sumathi et al, 2024).

Figura 15. *Principales características de SIDS.*

Fuente: adaptado de *(Sumathi et al, 2024). Elaboración propia utilizando Notebooklm (2026).*

Los sistemas de detección de intrusiones basados en anomalías (AIDS) identifican actividades maliciosas mediante la detección de desviaciones respecto al comportamiento normal de la red o del proceso industrial. Para ello, construyen modelos de referencia a partir de características del tráfico, variables de proceso o registros operativos, generando alertas cuando se observan comportamientos fuera de lo esperado. Su principal ventaja es la capacidad de detectar amenazas desconocidas, ataques de día cero y anomalías no registradas en bases de firmas tradicionales, como se muestra en la Figura 16. Sin embargo, suelen presentar mayores tasas de falsos positivos que los IDS basados en firmas y, al emplear modelos de aprendizaje automático que funcionan como "cajas negras", pueden dificultar la interpretación de las decisiones y reducir la confianza de los operadores en entornos industriales críticos (Skrodelis et al, 2025).

Figura 16. *Principales características de AIDS.*



Fuente: adaptado de *(Skrodelis et al, 2025). Elaboración propia utilizando Notebooklm (2026).*

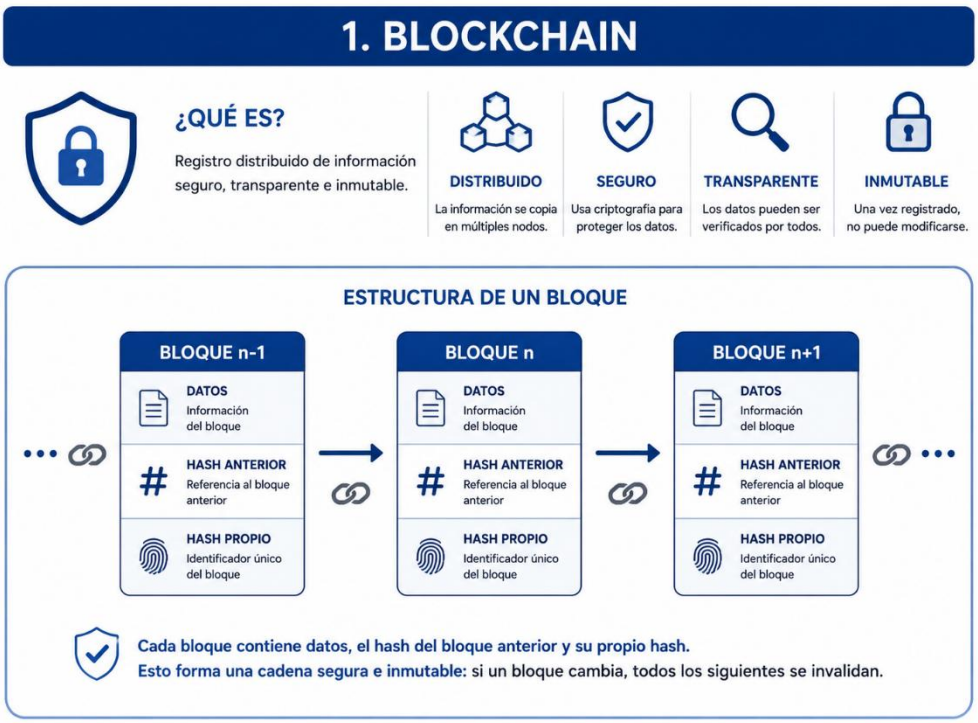
En fábricas inteligentes, se ha propuesto un IDS/IPS basado en aprendizaje profundo que utiliza una arquitectura BiLSTM con mecanismo de atención para detectar tráfico malicioso y comportamientos anómalos en redes industriales. El sistema, integrado mediante una API basada en Flask para operación en tiempo real, permite supervisar el tráfico de red y detectar ataques como la suplantación de direcciones IP con baja latencia. Los resultados alcanzaron una precisión de validación del 89.2 % y un puntaje F1 ponderado de 0.91, demostrando la viabilidad de las técnicas de inteligencia artificial para fortalecer la ciberseguridad en entornos de Industria 4.0 (Qurbani et al, 2025).

Otras investigaciones han orientado la aplicación de IDS en arquitecturas distribuidas de CPS e IIoT mediante técnicas de inteligencia de enjambre. En esta propuesta, el algoritmo Particle Swarm Optimization (PSO) selecciona las características más relevantes del tráfico de red para reducir la complejidad computacional y mejorar la clasificación, mientras que Ant Colony Optimization (ACO) correlaciona eventos sospechosos y reconstruye posibles rutas de propagación de ataques. La solución está diseñada para ejecutarse en capas edge y fog, donde los recursos son limitados y se requieren tiempos de respuesta reducidos. Los resultados muestran precisiones entre el 94 % y el 96 %, además de una disminución significativa de los falsos positivos frente a IDS convencionales (Swetha et al, 2025).

d) Blockchain y Deep learning

Blockchain es una tecnología de registro distribuido que permite almacenar información de forma segura, transparente e inmutable mediante una cadena de bloques enlazados criptográficamente (Almasabi et al, 1918), (Chandna et al, 2024). Cada bloque contiene información específica, un código hash propio y el hash del bloque anterior, lo que garantiza la integridad de los datos y dificulta cualquier modificación no autorizada (Almasabi et al, 1918) ver la figura 17.

Figura 17. *interpretación de la cadena de bloques Blockchain.*



Fuente: adaptado de *(Almasabi et al, 1918). Elaboración propia utilizando Notebooklm (2026).*

La tecnología blockchain puede clasificarse en redes públicas, privadas y de consorcio, según el nivel de acceso y participación permitido. Su funcionamiento se basa en la incorporación secuencial de bloques validados mediante mecanismos de consenso, como Proof of Work (PoW) y Proof of Stake (PoS), junto con funciones criptográficas como SHA-256 para garantizar la integridad de la información. En entornos SCADA e IIoT, blockchain se ha utilizado para fortalecer la seguridad, la integridad de los datos y la autenticación de dispositivos mediante arquitecturas que combinan blockchains públicas y privadas, contratos inteligentes y criptografía de clave pública. En redes eléctricas inteligentes, una implementación basada en Ethereum con Proof of Authority (PoA) demostró mejoras significativas en la confiabilidad de las comunicaciones, la integridad de los datos y la resiliencia frente a ataques como DoS e inyección de datos falsos (FDIA), validándose en topologías IEEE de 14, 30 y 118 barras (Almasabi, 1918).

En (Chandna et al, 2024) se integró blockchain con computación en la nube y sistemas SCADA para el monitoreo y supervisión de procesos industriales dentro del contexto de la

Industria 4.0. La propuesta utilizó blockchain como mecanismo de almacenamiento distribuido para proteger la información generada por sensores, controladores y dispositivos IoT, eliminando la dependencia de infraestructuras centralizadas. Los autores concluyeron que la combinación de blockchain, computación en la nube e inteligencia artificial contribuye a mejorar la seguridad, la confiabilidad y la digitalización de los procesos industriales (Chandna et al, 2024).

Por otra lado el Deep Learning es una rama del aprendizaje automático basada en redes neuronales artificiales profundas capaces de aprender automáticamente representaciones complejas a partir de grandes volúmenes de datos (Belayadi et al, 2025), (Cao et al, 2023). A diferencia de los métodos tradicionales de aprendizaje automático, estas técnicas permiten extraer características relevantes sin necesidad de definir manualmente los patrones de interés, lo que las hace especialmente adecuadas para entornos industriales con grandes cantidades de datos heterogéneos.

Entre las arquitecturas más utilizadas destacan las redes neuronales convolucionales (Convolutional Neural Networks, CNN), las redes neuronales (Red Neural Networks, RNN) y las redes Long Short-Term Memory (LSTM). Las CNN emplean filtros de convolución para identificar patrones espaciales complejos y son ampliamente utilizadas en tareas de clasificación y reconocimiento (Belayadi et al, 2025). Las RNN están diseñadas para procesar datos secuenciales considerando dependencias temporales entre las observaciones (Belayadi et al, 2025), (Cao et al, 2023). Por su parte, las redes LSTM constituyen una evolución de las RNN que incorporan mecanismos de memoria capaces de retener información durante períodos prolongados, lo que mejora significativamente el análisis de series temporales y tráfico de red industrial (Belayadi et al, 2025).

El funcionamiento general de los modelos Deep Learning comprende varias etapas: recopilación de datos, preprocesamiento, entrenamiento, validación y evaluación del modelo. Durante el entrenamiento, las redes neuronales ajustan automáticamente sus parámetros internos para minimizar errores de clasificación o predicción, permitiendo identificar patrones complejos asociados al comportamiento normal o anómalo de los sistemas industriales (Belayadi et al, 2025), (Cao et al, 2023).

La detección de intrusiones y actividades maliciosas constituye una de las aplicaciones más relevantes del Deep Learning en entornos SCADA e IIoT. En (Belayadi et al, 2025), se evaluaron arquitecturas CNN, RNN y LSTM utilizando los conjuntos de datos de referencia WUSTL-IIOT-2018 y WUSTL-IIOT-2021, ampliamente reconocidos en la investigación de ciberseguridad industrial por incorporar tráfico legítimo y escenarios de ataque representativos de infraestructuras IIoT. Los resultados evidenciaron un desempeño sobresaliente de las técnicas de aprendizaje profundo, alcanzando precisiones de hasta 99.99 % en la clasificación de amenazas. Particularmente, las arquitecturas CNN y LSTM superaron a las RNN, demostrando una mayor capacidad para identificar patrones complejos presentes en el tráfico industrial. Los modelos LSTM presentaron menores tasas de falsos positivos y falsos negativos, mientras que las CNN destacaron por su eficacia en la extracción automática de características relevantes para la detección de ataques. Estos resultados confirman el potencial del Deep Learning para fortalecer los sistemas de detección de intrusiones, proporcionando mecanismos más precisos, adaptativos y

robustos frente a las amenazas emergentes en infraestructuras SCADA e IIoT (Belayadi et al, 2025).

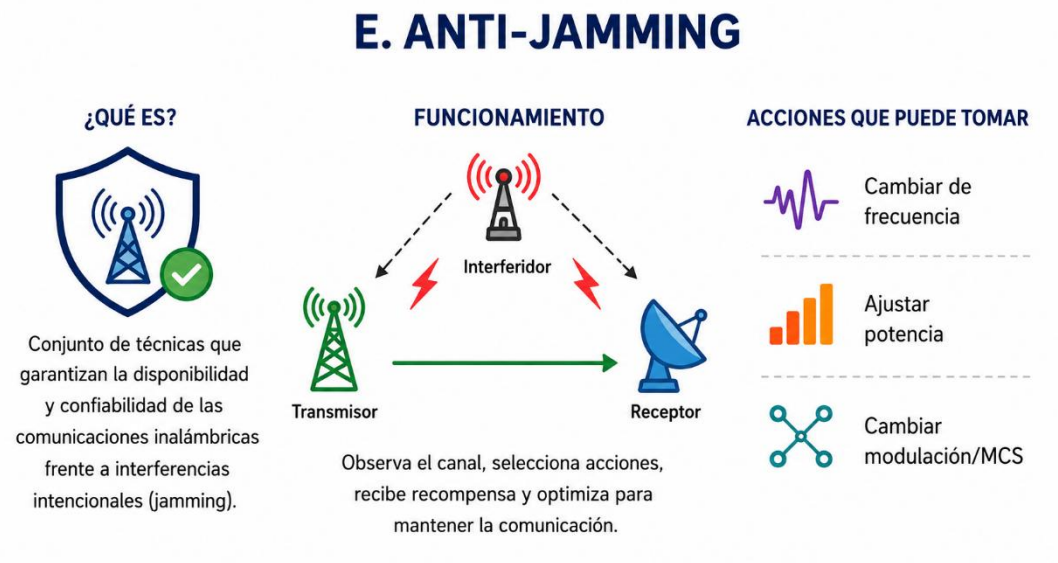
En (Cao et al, 2023) se desarrollaron modelos basados en redes neuronales artificiales (ANN) y redes neuronales recurrentes (RNN) para identificar actividades de ataque en entornos IIoT. La metodología incluyó la recopilación de datos de tráfico de red, el preprocesamiento de la información y el entrenamiento de los modelos mediante técnicas de aprendizaje profundo. Los autores concluyeron que las arquitecturas Deep Learning permiten detectar patrones complejos asociados a ciberataques y adaptarse a nuevas amenazas, constituyéndose en una alternativa prometedora para mejorar la ciberseguridad de infraestructuras industriales conectadas (Cao et al, 2023).

e) Anti- jamming

El anti-jamming son un conjunto de técnicas diseñadas para garantizar la disponibilidad y confiabilidad de las comunicaciones inalámbricas frente a ataques de interferencia intencional (jamming) (Cao et al, 2023), (Wei et al, 2026).

las técnicas anti-jamming han utilizado mecanismos de espectro ensanchado, tales como Frequency Hopping Spread Spectrum (FHSS) y Direct Sequence Spread Spectrum (DSSS). pero, el surgimiento de interferidores inteligentes capaces de aprender patrones de comunicación y adaptarse dinámicamente ha reducido la efectividad de estos métodos convencionales. Es por lo que las investigaciones recientes han incorporado técnicas de inteligencia artificial, particularmente aprendizaje por refuerzo profundo (Deep Reinforcement Learning, DRL), para desarrollar estrategias adaptativas capaces de responder en tiempo real a diferentes escenarios de interferencia (Cao et al, 2023) ver la figura 18.

Figura 18. *Descripción general de Anti Jamming.*



Fuente: adaptado de *(Cao et al, 2023). Elaboración propia utilizando Notebooklm (2026).*

El funcionamiento de un sistema anti-jamming se basa en la observación continua del estado del canal de comunicación y en la selección dinámica de acciones que permitan mantener la transmisión con niveles aceptables de desempeño. Generalmente, el sistema está compuesto por un transmisor, un receptor y uno o varios interferidores que intentan degradar la comunicación (Cao et al, 2023).

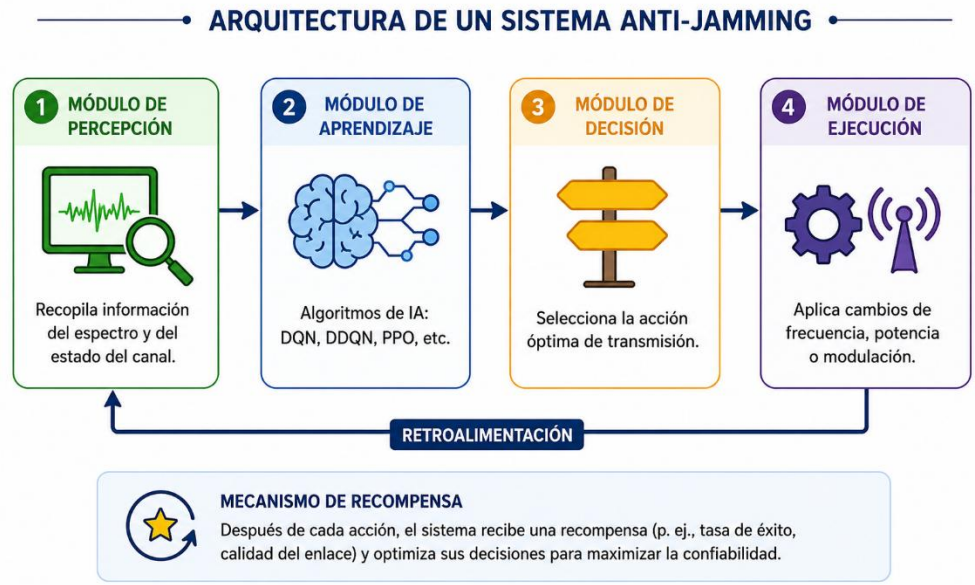
Después de cada acción, el sistema recibe una recompensa basada en métricas de desempeño, como la tasa de transmisión exitosa o la calidad del enlace. Mediante este mecanismo, los algoritmos de aprendizaje por refuerzo optimizan progresivamente las decisiones para maximizar la confiabilidad de la comunicación incluso bajo ataques de interferencia dinámicos (Cao et al, 2023), (Wei et al, 2026).

Los sistemas anti-jamming modernos suelen incorporar cuatro componentes principales (Cao et al, 2023), (Wei et al, 2026):

1. Módulo de percepción, encargado de recopilar información del espectro radioeléctrico y del estado del canal.
2. Módulo de aprendizaje, donde se implementan algoritmos de inteligencia artificial, como Deep Q-Network (DQN), Double Deep Q-Network (DDQN) o Proximal Policy Optimization (PPO).
3. Módulo de decisión, responsable de seleccionar la acción óptima de transmisión.
4. Módulo de ejecución, que aplica los cambios de frecuencia, potencia o modulación para mitigar la interferencia.

Por lo antes mencionado y como se muestra en la figura 19 esta arquitectura permite que el sistema se adapte automáticamente a nuevas estrategias de ataque sin necesidad de reglas predefinidas.

Figura 19. *Arquitectura de un sistema anti-jamming.*



Fuente: adaptado de *(Wei et al i, 2026). Elaboración propia utilizando Notebooklm (2026).*

Una aplicación relevante para redes inalámbricas inteligentes empleó un esquema anti-jamming basado en Double Deep Q-Network (DDQN) combinado con un Swin Transformer Block. En una red compuesta por transmisor, receptor e interferidor, el agente observaba continuamente el estado espectral del entorno y seleccionaba el canal y la potencia de transmisión más adecuados para mitigar la interferencia, utilizando aprendizaje por refuerzo profundo entrenado con datos obtenidos durante ataques tipo sawtooth sweep jammer. Los resultados mostraron una SINR de convergencia cercana a 13.8 dB tras 700 intervalos de tiempo, además de una convergencia más rápida y mayor estabilidad frente a ataques dinámicos en comparación con enfoques basados en CNN y Transformers convencionales, evidenciando una mejor capacidad de aprendizaje y adaptación del sistema anti-jamming (Cao et al, 2023).

Otra aplicación en comunicaciones satelitales desarrolló un mecanismo de asignación conjunta de recursos anti-jamming basado en aprendizaje por refuerzo profundo, optimizando simultáneamente la potencia de transmisión, la selección de canal y el esquema de modulación y codificación (MCS) bajo condiciones de desvanecimiento Rician e interferencia reactiva. Tras evaluar algoritmos como PPO, A2C y D3QN, PPO obtuvo el mejor desempeño en condiciones normales, alcanzando la mayor tasa útil de transmisión (goodput) y una probabilidad de interrupción nula. Sin embargo, ante escenarios extremos con incrementos de interferencia de hasta 40 dB, se propuso una variante denominada Robust-PPO, entrenada mediante domain randomization, que mejoró significativamente la resistencia frente a interferidores desconocidos, logrando un goodput de 1.75 bps/Hz, una reducción de la probabilidad de outage hasta 59.11 % y manteniendo una confiabilidad del 100 % en condiciones nominales (Wei et al, 2026).

Los resultados obtenidos en ambas investigaciones demuestran que la integración de técnicas de aprendizaje por refuerzo profundo permite desarrollar sistemas anti-jamming capaces de adaptarse dinámicamente a entornos hostiles, mejorando la robustez y disponibilidad de las comunicaciones inalámbricas frente a interferidores inteligentes (Cao et al, 2023), (Wei et al, 2026).

f) SDN y Network Slicing

La red definida por software (SDN) es un paradigma de gestión de redes que separa el plano de control del plano de datos, permitiendo que las decisiones de encaminamiento y administración se realicen de forma centralizada mediante un controlador programable. Esta arquitectura surge como respuesta a las limitaciones de las redes tradicionales, donde cada dispositivo administra de manera independiente sus funciones de control y reenvío, dificultando la gestión de entornos dinámicos y heterogéneos como el Internet Industrial de las Cosas (IIoT) (Khoa et al, 2022).

La estructura de SDN está compuesta principalmente por tres capas: el plano de aplicación, donde se implementan los servicios y políticas de red; el plano de control, representado por un controlador centralizado que toma decisiones de gestión; y el plano de datos, formado por los dispositivos de red encargados de reenviar el tráfico según las reglas establecidas por el controlador. La comunicación entre el controlador y los dispositivos de red suele realizarse

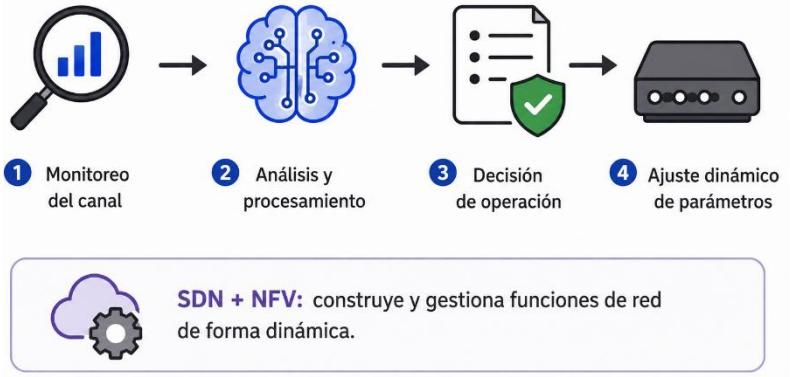
mediante protocolos como OpenFlow, que permiten modificar dinámicamente las tablas de flujo de los conmutadores (Khoa et al, 2022), ver la figura 20.

Figura 20. *Componentes de SDN.*

Fuente: adaptado de *(Khoa et al, 2022). Elaboración propia utilizando Notebooklm (2026).*

El funcionamiento de SDN se basa en la recopilación de información del estado de la red por parte del controlador, el análisis de dicha información y la generación de reglas de encaminamiento o seguridad que posteriormente son distribuidas a los dispositivos de la red. Gracias a esta separación funcional, SDN proporciona una administración más flexible, programable y escalable, facilitando la automatización de tareas de supervisión, detección de amenazas y aplicación de políticas de seguridad (Khoa et al, 2022), ver la figura 21.

Figura 21. *Flujo de operación de SDN.*



Fuente: adaptado de *(Khoa et al, 2022). Elaboración propia utilizando Notebooklm (2026).*

Además de sus aplicaciones en ciberseguridad, SDN constituye una de las tecnologías habilitadoras para las arquitecturas de red de nueva generación. La combinación de SDN con la virtualización de funciones de red (NFV) permite implementar arquitecturas orientadas a servicios,

donde las funciones de red pueden desplegarse, modificarse o escalarse dinámicamente según las necesidades operativas (Du et al, 2023).

Una aplicación de SDN para entornos IIoT propuso una estrategia de defensa proactiva basada en inteligencia de amenazas cibernéticas (CTI), donde indicadores de compromiso, como direcciones IP y dominios maliciosos, son obtenidos desde plataformas de intercambio de inteligencia y procesados automáticamente por un controlador SDN para generar reglas de seguridad OpenFlow. La implementación utilizó un controlador Ryu, conmutadores OpenFlow virtuales y un servidor MISP, permitiendo bloquear automáticamente tráfico asociado a amenazas antes de que alcanzara su destino. Los resultados demostraron la automatización eficiente de políticas de seguridad en redes IIoT de gran escala y evidenciaron que el modelo XGBoost alcanzó precisiones cercanas al 99 % en la detección de tráfico malicioso. Además, las pruebas de escalabilidad mostraron que la instalación de 100 reglas de bloqueo en una red con 10 conmutadores requirió aproximadamente 31,61 s y un uso de CPU cercano al 41 %, confirmando la viabilidad de la propuesta para aplicaciones industriales (Khoa et al, 2022).

Otra aplicación relacionada con SDN se presenta en (Du et al, 2023), donde se propone una arquitectura convergente basada en servicios (cSBA) para redes móviles de próxima generación. La propuesta utiliza los principios de SDN y NFV para desacoplar las funciones de acceso, control y transmisión de datos, permitiendo que los recursos de red se gestionen de forma flexible y programable.

La arquitectura propuesta divide la red en tres planos principales: acceso, encargado de conectar los dispositivos; control, responsable del procesamiento de señalización; y datos, dedicado al transporte de información. Además, incorpora interfaces basadas en servicios y mecanismos de gestión inteligente que ajustan dinámicamente los recursos según las condiciones de operación. Los resultados mostraron una mejora significativa frente a arquitecturas monolíticas tradicionales, manteniendo el mismo rendimiento con 21,75 núcleos de CPU frente a los 48 requeridos convencionalmente, lo que representa un ahorro del 45,31 %. Asimismo, en escenarios de tráfico creciente, la arquitectura basada en servicios alcanzó una capacidad de procesamiento al menos cinco veces superior utilizando la misma cantidad de recursos computacionales, evidenciando una mayor escalabilidad y eficiencia energética (Du et al, 2023).

g) Trust Evaluation Models

La gestión de confianza (Trust Management, TM) es un mecanismo de seguridad que evalúa continuamente el comportamiento de los nodos, dispositivos o usuarios de una red para determinar su nivel de confiabilidad y, con base en ello, permitir, restringir o revocar su acceso a los recursos del sistema (Stodt et al, 2023), (Mannix et al, 2024). A diferencia de los mecanismos tradicionales de seguridad basados únicamente en autenticación y cifrado, TM considera el comportamiento histórico y actual de las entidades para identificar actividades maliciosas que podrían pasar desapercibidas incluso después de una autenticación válida (Mannix et al, 2024).

En entornos IIoT, CPS e infraestructuras industriales distribuidas, la gestión de confianza resulta especialmente relevante debido al gran número de dispositivos conectados, la heterogeneidad de los equipos y la posibilidad de que nodos legítimos sean comprometidos por

atacantes (Stodt et al, 2023), (Mannix et al, 2024). Su objetivo principal es detectar entidades maliciosas o comprometidas y evitar que afecten la operación de la red.

El funcionamiento de un sistema de gestión de confianza se basa en la observación continua de las actividades realizadas por cada nodo de la red. A partir de estas observaciones se calcula una puntuación de confianza (trust score) que refleja el grado de confiabilidad de la entidad evaluada (Mannix et al, 2024).

Generalmente, el proceso consta de las siguientes etapas, ver la figura 22:

1. Monitoreo del comportamiento: se recopilan métricas relacionadas con las comunicaciones, calidad de los datos, cumplimiento de protocolos y comportamiento operativo de cada nodo.
2. Evaluación de confianza: las métricas obtenidas son procesadas mediante algoritmos de cálculo de confianza para generar una puntuación asociada a cada entidad.
3. Actualización dinámica: los valores de confianza son ajustados periódicamente según el comportamiento reciente y el historial acumulado.
4. Toma de decisiones: el sistema utiliza la puntuación de confianza para autorizar accesos, restringir privilegios, aislar dispositivos o expulsar nodos considerados maliciosos (Stodt et al, 2023), (Mannix et al, 2024).

Figura 22. *Resumen de las etapas TM.*

Fuente: adaptado de *(Stodt et al, 2023) (Mannix, 2024). Elaboración propia utilizando Notebooklm (2026).*

Este enfoque permite detectar amenazas internas, nodos comprometidos y ataques que no pueden identificarse únicamente mediante mecanismos criptográficos tradicionales.

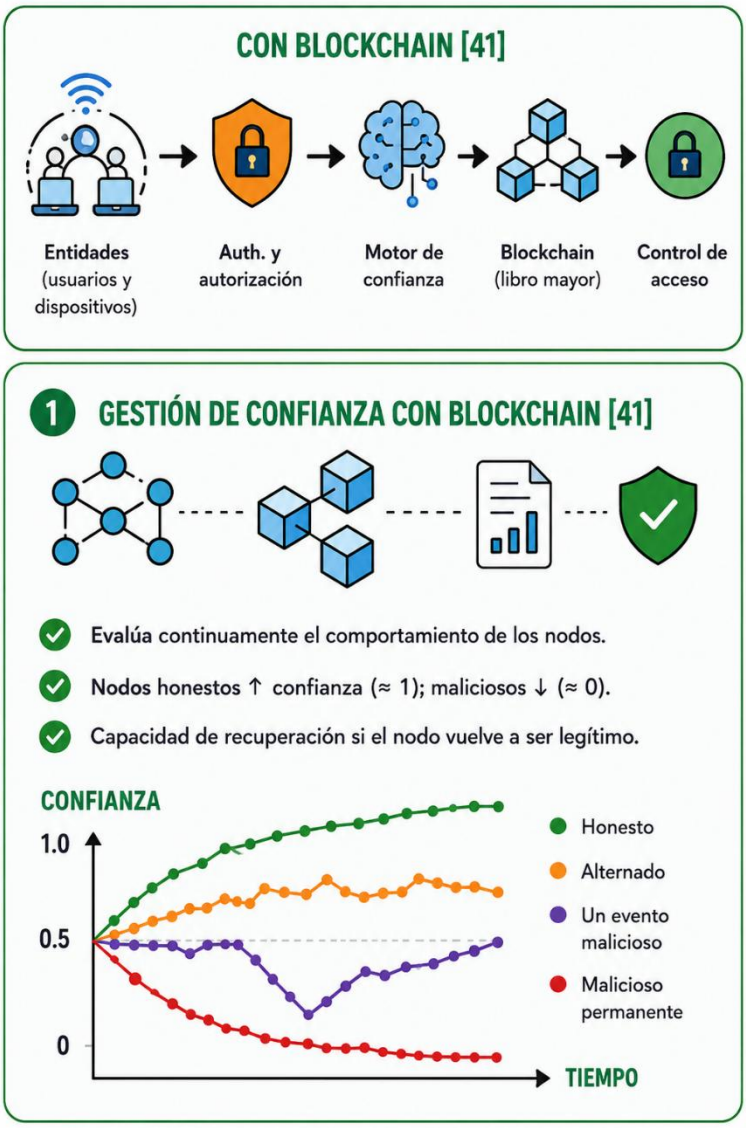
La arquitectura de un sistema TM suele estar compuesta por varios módulos funcionales encargados de recopilar información, calcular la confianza y aplicar políticas de seguridad, ver la figura 23.

En redes industriales basadas en blockchain, la estructura propuesta en (Stodt et al, 2023) incorpora:

- Entidades evaluadas (usuarios y dispositivos).
- Mecanismo de autenticación y autorización.
- Motor de cálculo de confianza.

- Blockchain o libro mayor distribuido para almacenar registros de confianza de forma inmutable.
- Módulo de control de acceso que utiliza los valores de confianza para autorizar o rechazar solicitudes.

Figura 23. *Funcionamiento de Trust Management con Blockchain.*



Fuente: adaptado de *(Stodt et al, 2023). Elaboración propia utilizando Notebooklm (2026).*

Por otro lado, en redes CPS e IoT tradicionales, la arquitectura presentada en (Mannix et al, 2024) está organizada jerárquicamente, donde los nodos recopilan información local y una estación base calcula los niveles de confianza utilizando parámetros de comportamiento y calidad de datos, ver figura 24.

Figura 24. *Esquema general de TM tradicional.*

Fuente: adaptado de *(Mannix et al, 2024). Elaboración propia utilizando Notebooklm (2026).*

En (Stodt et al, 2023) se desarrolló un sistema de gestión de confianza basado en blockchain para redes industriales híbridas. El objetivo fue evaluar continuamente la confiabilidad de los nodos participantes y utilizar dicha información para tomar decisiones de acceso.

El sistema empleó una infraestructura blockchain distribuida donde cada nodo recibe una puntuación de confianza inicial. Durante la operación, el comportamiento de los nodos es monitoreado y analizado periódicamente. En cada época de evaluación, el sistema calcula nuevos valores de confianza considerando factores como el historial de comportamiento, las acciones maliciosas detectadas y la reputación acumulada.

Para validar la propuesta se realizó una simulación con distintos perfiles de comportamiento:

- Un nodo mantuvo comportamiento malicioso permanente.
- Un nodo alternó entre comportamientos honestos y maliciosos.
- Otro nodo presentó un único episodio de comportamiento malicioso.
- Un nodo permaneció completamente honesto durante toda la simulación.

Los resultados mostraron que los nodos honestos incrementaron progresivamente su nivel de confianza hasta alcanzar valores cercanos a 1, mientras que los nodos maliciosos redujeron gradualmente su puntuación hasta valores próximos a 0. El sistema también demostró capacidad de recuperación, ya que los nodos que retornaban a un comportamiento legítimo recuperaban parcialmente su confianza después de varios ciclos de evaluación (Stodt et al, 2023).

Estos resultados evidencian que la integración de blockchain con mecanismos de gestión de confianza permite identificar eficazmente actores maliciosos y limitar su influencia dentro de redes industriales distribuidas.

En (Mannix et al, 2024) se propuso un modelo de gestión de confianza centrado en la monitorización de comunicaciones y datos para un sistema de gestión de agua basado en IoT.

La arquitectura consideró una red compuesta por sensores distribuidos geográficamente que reportaban información a una estación base central. El sistema calculó dos componentes principales de confianza:

- Trust de comunicaciones: evaluaba variaciones anómalas en la frecuencia de transmisión de paquetes.
- Trust de datos: analizaba la calidad de la información generada por cada nodo mediante un algoritmo de detección de anomalías basado en una máquina de vectores soporte de una clase (One-Class Online SVM).

Ambas métricas se combinaron para generar una puntuación global de confianza que era actualizada periódicamente mediante ventanas temporales deslizantes. Además, se implementó un umbral dinámico que se recalculaba continuamente según el comportamiento general de la red.

La validación experimental se realizó utilizando datos reales de sensores ambientales y de calidad del agua obtenidos de nueve ubicaciones costeras de Chicago. Posteriormente se introdujeron distintos ataques para evaluar el rendimiento del modelo.

En los ataques de comunicaciones se simularon pérdidas aleatorias de paquetes (packet dropping attacks). El sistema logró detectar comportamientos maliciosos incluso cuando la tasa de pérdida era tan baja como el 5% (Mannix et al, 2024).

En los ataques de datos se modificaron aleatoriamente las mediciones de sensores. El modelo identificó exitosamente alteraciones del 10% y 20% en los valores transmitidos por los nodos comprometidos (Mannix et al, 2024), ver la figura 25.

Figura 25. *Flujo de operación del modelo para IoT de tanque de agua.*

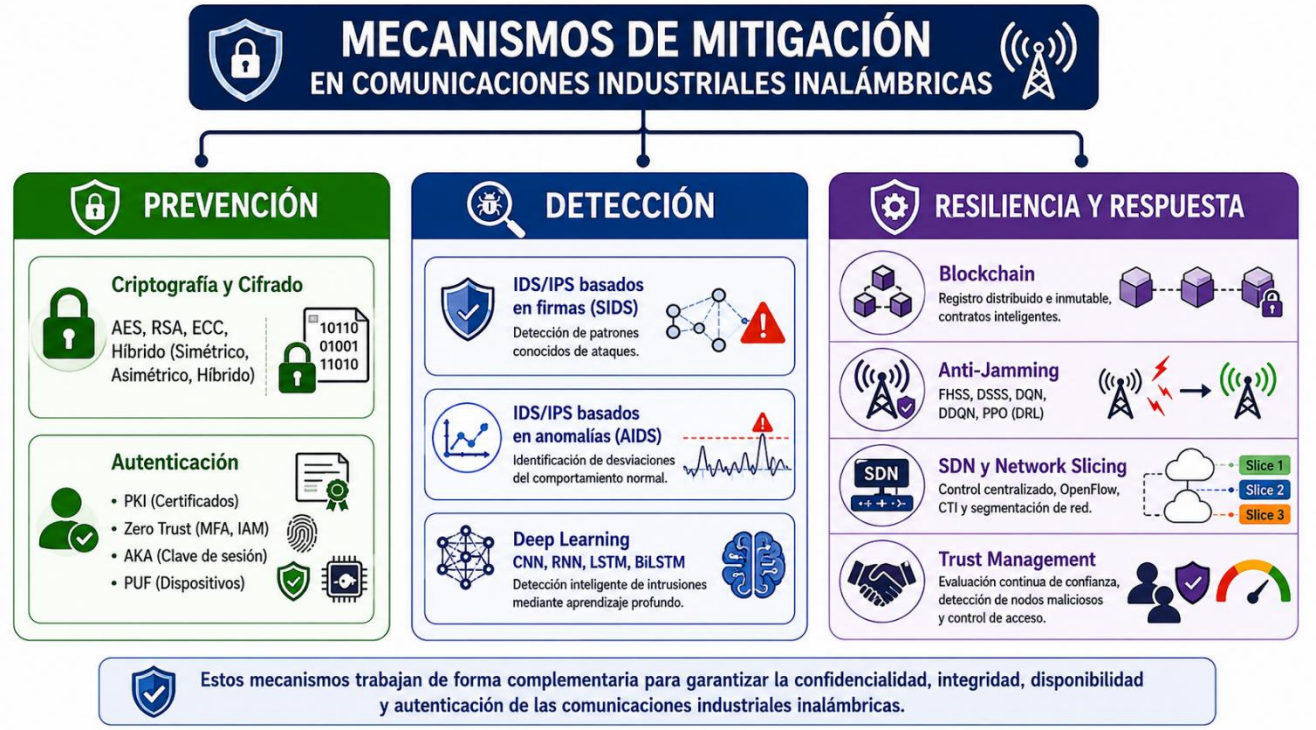
Fuente: adaptado de *(Mannix et al, 2024). Elaboración propia utilizando Notebooklm (2026).*

Los resultados mostraron una alta capacidad de detección sin generar falsos positivos durante las pruebas de control. Sin embargo, el rendimiento comenzó a degradarse cuando más de la mitad de los nodos de la red eran maliciosos, debido a que el mecanismo de cálculo del umbral dinámico empezaba a utilizar información proveniente de nodos comprometidos (Mannix et al, 2024).

En conjunto, estos resultados demuestran que los sistemas de gestión de confianza constituyen una solución eficaz para identificar comportamientos anómalos, detectar nodos comprometidos y reforzar la seguridad de redes IoT, CPS e infraestructuras industriales distribuidas.

Con el propósito de sintetizar los principales mecanismos de mitigación identificados en la literatura para la protección de las comunicaciones industriales inalámbricas, la Figura 26 presenta una clasificación general de las soluciones de ciberseguridad analizadas en esta revisión. Los mecanismos se agrupan en tres categorías funcionales: prevención, orientada a impedir accesos no autorizados y proteger la información mediante técnicas de criptografía y autenticación; detección, enfocada en la identificación de actividades maliciosas a través de sistemas IDS/IPS y algoritmos de aprendizaje profundo; y resiliencia y respuesta, destinada a garantizar la continuidad operativa y la capacidad de adaptación frente a amenazas mediante tecnologías como blockchain, sistemas anti-jamming, redes definidas por software (SDN) y modelos de gestión de confianza. Esta clasificación permite comprender cómo las diferentes estrategias de seguridad actúan de forma complementaria para preservar la confidencialidad, integridad, disponibilidad y autenticación en entornos IIoT, SCADA y comunicaciones industriales inalámbricas.

Figura 26. *Clasificación de los principales mecanismos de mitigación empleados en comunicaciones industriales inalámbricas.*



Elaboración propia utilizando Notebooklm (2026).

Relación entre amenazas y mecanismos de mitigación en redes inalámbricas industriales

El análisis de la literatura evidencia que la creciente adopción de protocolos inalámbricos en entornos industriales ha incrementado significativamente la superficie de ataque de las infraestructuras IIoT, CPS y SCADA. Como se mostró en las secciones anteriores, las amenazas pueden clasificarse en ataques contra la autenticación, integridad, confidencialidad y disponibilidad, afectando directamente los principios fundamentales de la ciberseguridad industrial.

Los resultados reportados en los diferentes estudios muestran que no existe un mecanismo universal capaz de mitigar todas las amenazas presentes en las redes industriales inalámbricas. Cada categoría de ataque requiere la implementación de una o varias estrategias de defensa. Los mecanismos criptográficos y de autenticación son especialmente efectivos frente a ataques de suplantación de identidad, repetición, interceptación y acceso no autorizado. Por su parte, los sistemas IDS/IPS y las técnicas basadas en Deep Learning permiten identificar comportamientos anómalos, intrusiones y amenazas desconocidas que no pueden ser detectadas únicamente mediante autenticación o cifrado. De forma similar, tecnologías como blockchain, SDN y los modelos de gestión de confianza aportan mecanismos adicionales de supervisión, control de acceso y validación del comportamiento de los dispositivos dentro de la red.

Tabla 2. *Relación entre ataques y mecanismos de mitigación.*

TIPO DE ATAQUE	EJEMPLO	DEFENSA
Autenticación	Spoofing Masquerade Replay Fuerza Bruta	Autenticación mutua PKI ZTA Blockchain Trust Management
Integridad	MITM Inyección de paquetes Manipulación de datos	Criptografía (AES, RSA, ECC) Blockchain IDS/IPS Deep Learning
Confidencialidad	Sniffing Eavesdropping Análisis de tráfico	Cifrado simétrico y asimétrico PKI Blockchain ZTA
Disponibilidad	DoS DDoS Jamming Flooding Packet Dropping	IDS/IPS SDN Anti-jamming DRL Trust Management
Amenazas internas	Nodos comprometidos comportamiento malicioso	Trust Management IDS basados en anomalías Deep Learning
Ataques desconocidos (Zero-Day)	Comportamientos no registrados previamente	IDS anomalías Machine Learning Deep Learning Trust Management

Nota: *esta tabla presenta un resume la relación observada entre los principales ataques identificados en la literatura y los mecanismos de mitigación más utilizados.*

También se observó una evolución en las estrategias de defensa utilizadas en redes industriales. Los mecanismos tradicionales basados únicamente en reglas estáticas, firmas o políticas predefinidas están siendo complementados por mecanismos capaces de aprender del comportamiento histórico de la red. Debido al aumento de ataques dinámicos y adaptativos que logran evadir las medidas de protección convencionales.

En este contexto, la inteligencia artificial y el aprendizaje automático se han convertido en elementos fundamentales de las arquitecturas modernas de ciberseguridad industrial. Diversas investigaciones utilizan registros históricos de tráfico, eventos de red, comportamiento de dispositivos y métricas operacionales para entrenar modelos capaces de identificar patrones anómalos, predecir amenazas y ajustar dinámicamente las estrategias de mitigación. Ejemplos de ello son los IDS basados en CNN, RNN y LSTM (Qurbani et al, 2025), (Belayadi et al, 2025), los sistemas anti-jamming basados en aprendizaje por refuerzo profundo (Cao et al, 2023), (Wei et al, 2026), los modelos de Trust Management sustentados en análisis de comportamiento (Stodt et al, 2023), (Mannix et al, 2024) y las soluciones SDN apoyadas por algoritmos de aprendizaje automático para la detección de tráfico malicioso (Khoa et al, 2022).

De manera general, puede observarse que la tendencia actual en ciberseguridad industrial está migrando desde modelos reactivos hacia mecanismos adaptativos e inteligentes. Estos sistemas no solo detectan incidentes una vez ocurridos, sino que utilizan información histórica para aprender continuamente del entorno, recalcular niveles de riesgo, actualizar políticas de seguridad y optimizar las respuestas frente a nuevas amenazas. Como consecuencia, las futuras arquitecturas de protección para redes inalámbricas industriales probablemente combinarán mecanismos tradicionales de seguridad, como criptografía y autenticación, con modelos avanzados de inteligencia artificial capaces de proporcionar capacidades predictivas y de adaptación en tiempo real.

Conclusiones

La revisión bibliográfica realizada confirma que las comunicaciones inalámbricas industriales se han convertido en un componente esencial de las arquitecturas IIoT, CPS y SCADA modernas. Sin embargo, el incremento de la conectividad y la integración entre tecnologías OT e IT ha ampliado significativamente la superficie de ataque, exponiendo los sistemas industriales a amenazas que afectan la autenticación, integridad, confidencialidad y disponibilidad de la información. La literatura analizada demuestra que los mecanismos tradicionales de seguridad, como la criptografía y la autenticación, continúan siendo fundamentales, pero resultan insuficientes cuando se utilizan de forma aislada frente a amenazas cada vez más sofisticadas y dinámicas.

Se identificó una tendencia creciente hacia la incorporación de mecanismos inteligentes basados en inteligencia artificial,

aprendizaje automático, blockchain y modelos de confianza, los cuales permiten complementar los enfoques tradicionales mediante capacidades de detección, adaptación y

respuesta en tiempo real. los trabajos revisados evalúan estas soluciones en entornos simulados o escenarios controlados.

Finalmente, se observa que las futuras líneas de investigación deberán orientarse hacia el desarrollo de arquitecturas de seguridad integradas capaces de combinar mecanismos criptográficos, autenticación, monitoreo inteligente y técnicas de aprendizaje adaptativo dentro de un mismo marco de protección y será necesario estudiar aspectos relacionados con la interoperabilidad entre tecnologías heterogéneas, la reducción del costo computacional en dispositivos con recursos limitados y la capacidad de respuesta frente a amenazas emergentes y ataques desconocidos. En este contexto, la convergencia entre ciberseguridad industrial e inteligencia artificial es un área con gran potencial para fortalecer la resiliencia de las redes inalámbricas industriales de próxima generación.

Referencias

[1] Achaal, B., Adda, M., Berger, M. et al. Study of smart grid cyber-security, examining architectures, communication networks, cyber-attacks, countermeasure techniques, and challenges. Cybersecurity 7, 10 (2024). https://doi.org/10.1186/s42400-023-00200-w.

[2] G. Singh Gaba, A. Sari, I. Butun, P. Singh, A. Gurtov and M. Liyanage, "A Survey on Security and Privacy of Industry 4.0 and Beyond: Technical Aspects, Use Cases, Challenges, and Research Directions," in IEEE Open Journal of the Communications Society, vol. 6, pp. 8865-8929, 2025, doi: 10.1109/OJCOMS.2025.3616289.

[3] J. Gan, C. Luo, W. Shi, Y. Liu, X. Liu and Z. Tian, "An Attack Exploiting Cyber-Arm Industry," in IEEE Transactions on Dependable and Secure Computing, vol. 22, no. 2, pp. 1686-1702, March-April 2025, doi: 10.1109/TDSC.2024.3451129.

[4] W. Feng, "A Review with a Novel Perspective on IoT Evolution, Technical Architecture, Applications, and Challenges-Solutions," 2025 IEEE 3rd International Conference on Image Processing and Computer Applications (ICIPCA), Shenyang, China, 2025, pp. 2161-2167, doi: 10.1109/ICIPCA65645.2025.11138143.

[5] P. Drahoš, E. Kučera, O. Haffner, R. Pribiš and L. Beňo, "Trends in Industrial Networks including APL, TSN, WiFi-6E and 5G Technologies," 2022 Cybernetics & Informatics (K&I), Visegrád, Hungary, 2022, pp. 1-7, doi: 10.1109/KI55792.2022.9925965.

[6] Marzieh Jalal Abadi; Babak Hossein Khalaj, "Connectivity through Wireless Communications and Sensors," in Industry 4.0 Vision for the Supply of Energy and Materials: Enabling Technologies and Emerging Applications , Wiley, 2022, pp.3-58, doi: 10.1002/9781119695868.ch1.

[7] S. Sheikhi et al., "Bridging Theory and Practice: Addressing Current Cybersecurity Gaps in Industry 5.0," in IEEE Access, vol. 13, pp. 92891-92905, 2025, doi: 10.1109/ACCESS.2025.3569130.

[8] A. A. J. Al-Abadi, M. B. Mohamed and A. Fakhfakh, "Impact Of Availability Attacks On Enabling IoT Based Healthcare Applications," 2023 International Wireless Communications and Mobile Computing (IWCMC), Marrakesh, Morocco, 2023, pp. 1666-1671, doi: 10.1109/IWCMC58020.2023.10183010.

[9] S. Zhao, Z. Lu and C. Wang, "Measurement Integrity Attacks Against Network Tomography: Feasibility and Defense," in IEEE Transactions on Dependable and Secure

Computing, vol. 18, no. 6, pp. 2617-2630, 1 Nov.-Dec. 2021, doi: 10.1109/TDSC.2019.2958934.

[10] S. Nirenjena and D. S. Baskaran, "An Investigation on Distributed Denial of Service Attack in Edge Computing," 2023 5th International Conference on Smart Systems and Inventive Technology (ICSSIT), Tirunelveli, India, 2023, pp. 668-675, doi: 10.1109/ICSSIT55814.2023.10061128.

[11] L. Kapicak, J. Stipal, K. Trubak, P. Machnik and P. L. Si, "Detection System for Passive Network Eavesdropping," 2024 15th IFIP Wireless and Mobile Networking Conference (WMNC), Venice, Italy, 2024, pp. 41-46, doi: 10.52545/3-6.

[12] A. Sharma, H. Babbar and A. K. Vats, "Empowering Security: Machine Learning Solutions for Detecting Brute Force Attacks," 2024 4th Asian Conference on Innovation in Technology (ASIANCON), Pimari Chinchwad, India, 2024, pp. 1-5, doi: 10.1109/ASIANCON62057.2024.10838096.

[13] K. P. Swain, A. Tiwari, A. Sharma, S. Chakrabarti and A. Karkare, "Comprehensive Demonstration of Man-in-the-Middle Attack in PDC and PMU Network," 2022 22nd National Power Systems Conference (NPSC), New Delhi, India, 2022, pp. 213-217, doi: 10.1109/NPSC57038.2022.10069874.

[14] L. Dolai, P. Maity, T. Jana, P. Sadhu, T. Adhikari and S. Ghosal, "Securing Software Defined Networks from Packet Injection Attacks: A Framework for Detection and Prevention," 2025 2nd International Conference on Computational Intelligence, Communication Technology and Networking (CICTN), Ghaziabad, India, 2025, pp. 783-788, doi: 10.1109/CICTN64563.2025.10932605.

[15] R. Shaw and S. Parveen, "Literature Review on Packet Sniffing: Essential for Cybersecurity & Network Security," 2024 5th International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV), Tirunelveli, India, 2024, pp. 715-719, doi: 10.1109/ICICV62344.2024.00119.

[16] H. Pirayesh and H. Zeng, "Jamming Attacks and Anti-Jamming Strategies in Wireless Networks: A Comprehensive Survey," in IEEE Communications Surveys & Tutorials, vol. 24, no. 2, pp. 767-809, Secondquarter 2022, doi: 10.1109/COMST.2022.3159185.

[17] Jupriyadi, R. M. Negara, E. Mulyana and N. R. Syambas, "The Impact of Collusive Interest Flooding Attack on NDN Network Performance," 2024 10th International Conference on Wireless and Telematics (ICWT), Batam, Indonesia, 2024, pp. 1-5, doi: 10.1109/ICWT62080.2024.10674740.

[18] V. Kodela, N. N. Gadani, S. Chandramohan, P. K. Pareek, V. Veeramachaneni and M. G. Kumar, "Cybersecurity and Cryptography Protecting Information in the Digital Age," 2025 13th International Conference on Smart Grid (icSmartGrid), Glasgow, United Kingdom, 2025, pp. 489-495, doi: 10.1109/icSmartGrid66138.2025.11071738.

[19] Z. Wang, "Research on edge data Processing security technology in Industrial Internet," 2022 3rd International Conference on Computer Vision, Image and Deep Learning & International Conference on Computer Engineering and Applications (CVIDL & ICCEA), Changchun, China, 2022, pp. 1102-1108, doi: 10.1109/CVIDLICCEA56201.2022.9824602.

[20] R. Sokullu, "LoRa Based Smart Agriculture Network," 2022 8th International Conference on Energy Efficiency and Agricultural Engineering (EE&AE), Ruse, Bulgaria, 2022, pp. 1-4, doi: 10.1109/EEAE53789.2022.9831210.

[21] M. Haka, A. Haka, V. Aleksieva and H. Valchanov, "An Approach to Network Key Encryption in the Zigbee Network for IoT," 2025 International Conference Automatics and Informatics (ICAI), Varna, Bulgaria, 2025, pp. 543-548, doi: 10.1109/ICAI67591.2025.11324567.

[22] D. Yin and B. Gong, "A Lightweight Certificateless Mutual Authentication Scheme Based on Signatures for IIoT," in IEEE Internet of Things Journal, vol. 11, no. 16, pp. 26852-26865, 15 Aug.15, 2024, doi: 10.1109/JIOT.2024.3389018.

[23] Y. Lu, X. Chen and C. Chen, "Security authentication mechanism based on symmetric polynomials for SCADA systems," 2016 International Conference on Security of Smart Cities, Industrial Control System and Communications (SSIC), Paris, France, 2016, pp. 1-6, doi: 10.1109/SSIC.2016.7571806.

[24] A. A. Krishnan, S. K. Rajendran and T. K. Sunil Kumar, "Improved PKI Certificate Lifecycle Management With Centralized Device Management For Industrial IoT," 2022 IEEE International Conference on Public Key Infrastructure and its Applications (PKIA), Bangalore, India, 2022, pp. 1-5, doi: 10.1109/PKIA56009.2022.9952216.

[25] L. Kumar, K. S. Sisodiya Bais and S. Lata, "Securing Industrial IoT with Zero Trust: A Framework for Critical Infrastructure," 2025 International Conference on Information, Implementation, and Innovation in Technology (I2ITCON), Pune, India, 2025, pp. 1-5, doi: 10.1109/I2ITCON65200.2025.11210610.

[26] A. Singh, R. K. Dhanaraj, A. K. Sharma, B. Balusamy, G. Sharma and S. Agrawal, "Q-Learning Based Network Access Policy Management for Zero Trust Security in IIoT," 2023 International Conference on Electrical, Electronics, Communication and Computers (ELEXCOM), Roorkee, India, 2023, pp. 1-5, doi: 10.1109/ELEXCOM58812.2023.10370294.

[27] R. Cheng, "A Zero-Trust based Security Protection Scheme for Industrial IoT," 2025 7th International Conference on Frontier Technologies of Information and Computer (ICFTIC), Qingdao, China, 2025, pp. 986-989, doi: 10.1109/ICFTIC68075.2025.11324911.

[28] G. Abdelhady, A. Ghandoura, A. Motwakel and A. Alajmi, "Hybrid Machine Learning Anomaly Detection and Lightweight Zero Trust Authentication for LoRaWAN Networks," in IEEE Access, vol. 14, pp. 18387-18407, 2026, doi: 10.1109/ACCESS.2026.3660731.

[29] S. Yu and Y. Park, "A Modeling Attack-Resistant PUF-Enabled Robust Authentication and Key Agreement Scheme for Industrial Wireless Sensor Networks," in IEEE Internet of Things Journal, vol. 13, no. 10, pp. 21825-21840, 15 May15, 2026, doi: 10.1109/JIOT.2026.3667421.

[30] A. M, G. Sumathi, M. G., V. K. D., A. M. C. and R. Rajendran, "Enhancing Intrusion Detection in IIoT Environments: A Scalable and Economical Approach with Metric Active Learning," 2024 Second International Conference on Intelligent Cyber Physical Systems and Internet of Things (ICoICI), Coimbatore, India, 2024, pp. 1-6, doi: 10.1109/ICoICI62503.2024.10696440.

[31] H. K. Skrodelis, A. Romanovs and A. Lieknins, "Explainable SCADA Hybrid IDS: Gaps and Hypothesis," 2025 66th International Scientific Conference on Information Technology and Management Science of Riga Technical University (ITMS), Riga, Latvia, 2025, pp. 1-5, doi: 10.1109/ITMS67030.2025.11236701.

[32] S. Qurbani, A. M. Ramly, P. S. Chakolthi and M. S. Sharif, "An Intelligent IDS/IPS Framework to Fortify Industry 4.0 Applications," 2025 International Conference on

Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT), Sakhir, Bahrain, 2025, pp. 1-5, doi: 10.1109/3ict68299.2025.11442001.

[33] S. A, S. B. S, V. R. N, L. M. C, S. S and P. R, "Hybrid Optimization Based Intrusion Detection System Using Bio Inspired Algorithms for CPS in Industrial IoT," 2025 International Conference on Circuits, Controls and Communications (CCUBE), Bangalore, India, 2025, pp. 1-5, doi: 10.1109/CCUBE66458.2025.11340303.

[34] S. Almasabi, A. Shaf, T. Ali, M. Zafar, M. Irfan and T. Alsuwian, "Securing Smart Grid Data With Blockchain and Wireless Sensor Networks: A Collaborative Approach," in IEEE Access, vol. 12, pp. 19181-19198, 2024, doi: 10.1109/ACCESS.2024.3361752.

[35] M. Chandna, "Monitoring and Prediction of Supervision System for Industrial and Manufacturing Sectors Using Cloud Computing and Blockchain Technology," 2024 International Conference on Communication, Computer Sciences and Engineering (IC3SE), Gautam Buddha Nagar, India, 2024, pp. 1-6, doi: 10.1109/IC3SE62002.2024.10592888.

[36] D. Belayadi, H. Lebkara, N. Ouar and K. Lakhdari, "Leveraging Deep Learning for Cyberattack Detection: Advancing SCADA System Security in the IIoT Era," 2025 7th International Conference on Pattern Analysis and Intelligent Systems (PAIS), Laghouat, Algeria, 2025, pp. 1-7, doi: 10.1109/PAIS66004.2025.11126472.

[37] K. Cao and H. Zhengkong, "Intelligent anti-jamming methods for wireless networks," 2023 8th International Conference on Intelligent Computing and Signal Processing (ICSP), Xi'an, China, 2023, pp. 670-674, doi: 10.1109/ICSP58490.2023.10248518

[38] J. Wei, Y. Tian, G. Zhao, W. Zhang, H. Li and Y. Wang, "Robust PPO for Anti-Jamming Satellite Communications: Strong In-Distribution Performance and Improved Extreme-Jammer Generalization," 2026 IEEE 8th International Conference on Communications, Information System and Computer Engineering (CISCE), Guangzhou, China, 2026, pp. 309-313, doi: 10.1109/CISCE69494.2026.11504956.

[39] N. H. Khoa et al., "Cyber Threat Intelligence for Proactive Defense against Adversary in SDN-assisted IIoTs context," 2022 RIVF International Conference on Computing and Communication Technologies (RIVF), Ho Chi Minh City, Vietnam, 2022, pp. 1-6, doi: 10.1109/RIVF55975.2022.10013811.

[40] K. Du, L. Wang, Z. Zhu, Y. Yan and X. Wen, "Converged Service-based Architecture for Next-Generation Mobile Communication Networks," 2023 IEEE Wireless Communications and Networking Conference (WCNC), Glasgow, United Kingdom, 2023, pp. 1-6, doi: 10.1109/WCNC55385.2023.10118793.

[41] F. Stodt, C. Reich, A. Sikora and D. Welte, "Trust Management System for Hybrid Industrial Blockchains," 2023 IEEE 21st International Conference on Industrial Informatics (INDIN), Lemgo, Germany, 2023, pp. 1-6, doi: 10.1109/INDIN51400.2023.10218183.

[42] K. Mannix, A. Gorey, D. O'Shea and T. Newe, "Trust Management for Cyber Physical Systems and IoT Networks: New Communications and Data Centric Model," 2024 35th Irish Signals and Systems Conference (ISSC), Belfast, United Kingdom, 2024, pp. 1-6, doi: 10.1109/ISSC61953.2024.10603006.

[43] C. Schmittner, A. M. Shaaban and G. Macher, "ThreatGet: Ensuring the Implementation of Defense-in-Depth Strategy for IIoT Based on IEC 62443," 2022 IEEE 5th International Conference on Industrial Cyber-Physical Systems (ICPS), Coventry, United Kingdom, 2022, pp. 1-6, doi: 10.1109/ICPS51978.2022.9816864.