**Antecedentes**

Kushwaha et al. (2025) presentan una revisión exhaustiva de los Sistemas de Detección de Intrusos (IDS) inteligentes para la seguridad del Internet de las Cosas (IoT), enfocándose en soluciones que utilizan Inteligencia Artificial (IA), Aprendizaje Automático (ML) y Aprendizaje Profundo (DL). El estudio destaca que, si bien los dispositivos IoT han transformado diversas industrias, sus limitaciones inherentes de recursos como almacenamiento y capacidad computacional los exponen a ciberamenazas significativas. Los mecanismos de seguridad tradicionales, como los firewalls, a menudo resultan insuficientes para proteger estos dispositivos. La investigación analiza los enfoques de IDS existentes en las capas de borde, niebla y nube, señalando sus fortalezas y debilidades, e identifica desafíos clave como la complejidad computacional y la adaptabilidad en tiempo real, factores que impactan directamente en la precisión de la clasificación del tráfico de red.

Sahoo et al. (2026) abordan la necesidad de mejorar la fidelidad y explicabilidad de los IDS basados en ML en entornos de borde-IoT, proponiendo el marco de aprendizaje federado denominado Choir-IDS. El estudio señala que, aunque los modelos de ML son prometedores para la detección de intrusiones, su precisión puede ser inconsistente y a menudo requieren grandes cantidades de datos etiquetados para un entrenamiento efectivo. Choir-IDS utiliza un enfoque de "Neural Boosting Ensembles", que combina sinérgicamente el aprendizaje profundo con técnicas de ensamblaje para potenciar el rendimiento de la detección. Además, integra técnicas avanzadas de calibración (isotónica y sigmoide) para garantizar estimaciones de probabilidad precisas y herramientas de explicabilidad como LIME y SHAP para aumentar la transparencia y la confianza en el modelo, estableciendo un nuevo punto de referencia para IDS fiables y explicables.

Por su parte, Shenfield et al. (2018) presentan un enfoque novedoso para la detección de tráfico de red malicioso, específicamente *shellcode*, utilizando redes neuronales artificiales (ANN). Su investigación demuestra que una arquitectura de ANN bien diseñada, en su caso un perceptrón multicapa (MLP) con dos capas ocultas, puede distinguir con alta precisión entre tráfico benigno y malicioso. Los resultados experimentales, validados mediante validación cruzada repetida de 10 pliegues, muestran una precisión promedio del 98% y una tasa de falsos positivos inferior al 2% en un conjunto de datos a gran escala. Este trabajo subraya el potencial de las ANN para lograr una alta precisión de clasificación, minimizando los falsos positivos, un problema común en los sistemas basados en firmas tradicionales.

Gueriani et al. (2025) proponen un sistema de detección de intrusiones (IDS) robusto y de dominio cruzado, denominado BiGAT-ID, que utiliza un modelo híbrido de aprendizaje profundo que combina unidades recurrentes cerradas bidireccionales (BiGRU), memoria a corto-largo plazo (LSTM) y atención multicabeza (MHA). El modelo fue diseñado para operar eficazmente tanto en entornos de IoT Médico (IoMT) como de IoT Industrial (IIoT), demostrando una alta robustez y capacidad de generalización. En experimentos con los conjuntos de datos CICIoMT2024 y EdgeIIoTset, BiGAT-ID alcanzó precisiones de detección del 99.13% y 99.34%, respectivamente, con tiempos de inferencia extremadamente bajos. Este estudio resalta cómo arquitecturas de aprendizaje profundo complejas y sinérgicas pueden lograr una clasificación casi perfecta, abordando directamente el problema de la baja precisión en ecosistemas IoT heterogéneos.

Lebedev y Rzayev (2023) proponen un método para mejorar la calidad de los clasificadores de tráfico de red a través de la segmentación de datos. La premisa es que el tráfico de red no es homogéneo y las propiedades de los datos pueden cambiar con el tiempo debido a factores externos. En lugar de utilizar un único clasificador para todo el conjunto de datos, sugieren dividir la muestra de datos en segmentos no intersecantes y asignar a cada segmento el algoritmo de clasificación que demuestre el mejor rendimiento para sus características específicas. Este enfoque permite adaptar el proceso de clasificación a las condiciones cambiantes y a la heterogeneidad del tráfico, lo que puede aumentar los indicadores de calidad de la clasificación y combatir problemas como la dispersión de respuestas que afectan negativamente la precisión.

En una evaluación comparativa, Arabiat y Altayeb (2024) investigaron el rendimiento de varios clasificadores de aprendizaje automático para la predicción de ataques en entornos IoT, utilizando el conjunto de datos RT-IoT2022. El estudio construyó un modelo en la herramienta de minería de datos Orange3 para evaluar cuatro algoritmos: Random Forest (RF), Red Neuronal Artificial (ANN), Regresión Logística (LR) y Máquina de Vectores de Soporte (SVM). Los resultados experimentales demostraron una superioridad clara del clasificador Random Forest, que alcanzó una precisión de clasificación del 99.9%, superando significativamente a los otros modelos como ANN (99.8%), LR (97.8%) y SVM (92.9%). Este trabajo evidencia que la elección del algoritmo clasificador es un factor crítico para alcanzar una alta precisión en la detección de ataques IoT.

Kareem et al. (2023) se enfocaron en la detección de ataques de escaneo de puertos (PortScan) utilizando técnicas de aprendizaje automático, destacando el clasificador JRip, un algoritmo basado en reglas. La investigación subraya la importancia de la selección de características para mejorar la precisión y la eficiencia del modelo, utilizando un método híbrido basado en el filtrado por varianza y la ratio de ganancia de información para reducir el número de atributos de 84 a 13. Al entrenar y probar el modelo con el conjunto de datos CICIDS2017, el esquema de detección basado en JRip alcanzó una precisión del 99.84% con una sobrecarga de detección muy baja. Este estudio demuestra que un algoritmo basado en reglas, combinado con una selección de características eficaz, puede lograr una clasificación de alta precisión para tipos de ataques específicos.

Al-Khazaali et al. (2025) investigan las características específicas del tráfico de escaneo de puertos generado por la herramienta Nmap, con el objetivo de identificar patrones que puedan ser utilizados para desarrollar sistemas de detección de intrusiones más efectivos. En lugar de proponer un clasificador, su contribución se centra en la ingeniería de características, introduciendo el concepto de "Indicador de Escaneo" (IoS). Estos indicadores incluyen atributos como la distribución de puertos de origen y destino, la duración del escaneo, el tamaño y número de paquetes, y medidas estadísticas asociadas. El estudio sugiere que estos IoS pueden servir como huellas digitales para detectar no solo la actividad de escaneo, sino también para identificar la herramienta específica utilizada, lo que demuestra que una comprensión profunda del comportamiento del tráfico es crucial para mejorar la precisión de la clasificación.

Guo et al. (2025) proponen una innovadora tecnología de seguridad de red anti-mapeo para contrarrestar los escaneos ilegales, utilizando un modelo Bi-LSTM con un mecanismo de atención (Bi-LSTM+Attention). El estudio destaca que los escaneos de red son precursores de ciberataques más graves y que las defensas estáticas son insuficientes. Al validar su modelo en el conjunto de datos UNSW-NB15, lograron una precisión del 98% y una reducción de la tasa de falsas alarmas en un 30% en comparación con un modelo LSTM tradicional. Este trabajo resalta cómo las arquitecturas avanzadas de aprendizaje profundo, que pueden capturar dependencias temporales bidireccionales y enfocarse en características relevantes, son capaces de mejorar significativamente la precisión y fiabilidad de los sistemas de detección.

Finalmente, Jafarian et al. (2023) presentan un enfoque proactivo para detectar escaneos de red, tanto internos como externos, que se basa en la correlación de los flujos de red con las consultas DNS precedentes y la manipulación de los valores TTL de los registros DNS. El principio fundamental es que una conexión legítima a una dirección IP generalmente debe estar precedida por una consulta DNS para resolver esa IP. Al reducir los valores de TTL, se obliga a realizar consultas DNS más frecuentes, lo que dificulta que los atacantes se aprovechen de los registros DNS en caché para evadir la detección. En un entorno de prueba, este método alcanzó una precisión superior al 96% y demostró ser eficaz incluso contra escáneres sigilosos y adaptativos. Este enfoque muestra que la incorporación de lógica de políticas y contexto de red puede ser una estrategia poderosa para complementar los modelos de clasificación y mejorar su precisión.

**Referencias**

**Al-Khazaali, Z., Al-Ghabban, A., Al-Musawi, H., Sabah, A., & Al Mahdi, N. (2025). Characteristics of Port Scan Traffic: A Case Study Using Nmap. *Journal of Engineering and Applied Science Development*, *29*(1). https://doi.org/10.31272/jeasd.2638**

**Arabiat, A., & Altayeb, M. (2024). Enhancing internet of things security: evaluating machine learning classifiers for attack prediction. *International Journal of Electrical and Computer Engineering (IJECE)*, *14*(5), 6036-6046. https://doi.org/10.11591/ijece.v14i5.pp6036-6046**

**Gueriani, A., Kheddar, H., Mazari, A. C., & Ghanem, M. C. (2025). A robust cross-domain IDS using BiGRU-LSTM-attention for medical and industrial IoT security. *ICT Express*. https://doi.org/10.1016/j.icte.2025.08.011**

**Guo, M., Ma, D., Jing, F., Zhang, X., & Liu, H. (2025). Dynamic Anti-Mapping Network Security Using Hidden Markov Models and LSTM Networks Against Illegal Scanning. *Informatica*, *49*, 207-220.**

**Jafarian, J. H., Abolfathi, M., & Rahimian, M. (2023). Detecting Network Scanning Through Monitoring and Manipulation of DNS Traffic. *IEEE Access*, 1-20. https://doi.org/10.1109/ACCESS.2023.3250106**

**Kareem, M. I., Abood, M. J. K., & Ibrahim, K. (2023). Machine learning-based PortScan attacks detection using OneR classifier. *Bulletin of Electrical Engineering and Informatics*, *12*(6), 3690-3696. https://doi.org/10.11591/eei.v12i6.4142**

**Kushwaha, J. P., Bhadauria, S., & Tapaswi, S. (2025). Unveiling IoT ecosystem security: A review of intelligent IDS, rends, challenges, and future directions. *Computers and Electrical Engineering*, *128*, 110626. https://doi.org/10.1016/j.compeleceng.2025.110626**

**Lebedev, I., & Rzayev, B. (2023). Segmentation of data when analyzing the state of telecommunication systems. *Indonesian Journal of Electrical Engineering and Computer Science*, *29*(3), 1473-1479. https://doi.org/10.11591/ijeecs.v29.i3.pp1473-1479**

**Sahoo, J. P., Kar, B., Abdelmoniem, A. M., & Chatzopoulos, D. (2026). Choir-IDS: A federated learning framework for fidelity-calibrated explainable intrusion detection system for edge-IoT networks. *Information Fusion*, *125*, 103473. https://doi.org/10.1016/j.inffus.2025.103473**

**Shenfield, A., Day, D., & Ayesh, A. (2018). Intelligent intrusion detection systems using artificial neural networks. *ICT Express*, *4*, 95-99. https://doi.org/10.1016/j.icte.2018.04.003**