**Antecedentes**

El incremento exponencial de dispositivos del Internet de las Cosas (IoT), que se proyecta alcanzará los 55.7 mil millones para el año 2025, ha transformado la vida cotidiana y diversas industrias. Sin embargo, la naturaleza de recursos limitados de estos dispositivos (almacenamiento, capacidad computacional y batería) los expone a una amplia gama de ciberamenazas, haciendo insuficientes los mecanismos de seguridad tradicionales como los firewalls. En este contexto, los Sistemas de Detección de Intrusiones (IDS) inteligentes, que emplean Inteligencia Artificial (IA), Aprendizaje Automático (ML) y Aprendizaje Profundo (DL), han emergido como soluciones efectivas para la seguridad en IoT. La investigación destaca la necesidad urgente de IDS ligeros y adaptativos que puedan manejar la complejidad computacional, la adaptabilidad en tiempo real y la eficiencia energética, y propone futuras direcciones como los IDS autoevolutivos y el aprendizaje continuo para enfrentar ataques sofisticados y en constante evolución.

En el ámbito de la seguridad para redes Edge-IoT, Sahoo et al. (2026) introducen Choir-IDS, un innovador marco de aprendizaje federado (FL) diseñado para optimizar la fidelidad y la explicabilidad de los sistemas de detección de intrusiones (IDS). Este enfoque combina la sinergia de múltiples modelos de Machine Learning y Deep Learning mediante sus "Neural Boosting Ensembles", lo que permite una detección robusta y escalable en entornos descentralizados. La fidelidad, en este contexto, se define como la capacidad del modelo para representar con precisión la verdad fundamental de los incidentes de seguridad y clasificar correctamente las amenazas sin generar falsos positivos o negativos. Además, la integración de herramientas de explicabilidad como LIME y SHAP mejora la transparencia y la confianza en las decisiones del modelo. Evaluado en conjuntos de datos como UNSW-NB15 y CICIoT2023, Choir-IDS demuestra una mejora notable en el rendimiento de detección, incluso en condiciones de datos no distribuidos de manera independiente e idéntica (non-IID).

Shenfield et al. (2018) proponen un enfoque innovador para la detección de tráfico de red malicioso utilizando redes neuronales artificiales (ANN), específicamente adaptadas para sistemas de detección de intrusiones (IDS) basados en la inspección profunda de paquetes. Su estudio muestra que la arquitectura ANN propuesta puede distinguir con precisión entre tráfico de red benigno y malicioso, logrando una precisión promedio del 98% y una tasa de falsos positivos inferior al 2% en validaciones cruzadas repetidas de 10 pliegues. A diferencia de los sistemas basados en firmas, que resultan ineficaces contra amenazas desconocidas o modificadas y a menudo generan altas tasas de falsos positivos, el método basado en ANN es auto-adaptativo y no depende de firmas, permitiéndole capturar relaciones complejas y no lineales en los datos sin requerir conocimiento previo del modelo de probabilidad subyacente. Esta capacidad es particularmente crucial para la detección de shellcode, una amenaza de alto impacto que los métodos tradicionales a menudo no logran diferenciar del tráfico benigno.

Gueriani et al. (2025) abordan los complejos desafíos de ciberseguridad en el Internet de las Cosas Médicas (IoMT) y el Internet Industrial de las Cosas (IIoT) mediante la introducción de BiGAT-ID, un sistema de detección de intrusiones (IDS) novedoso basado en transformadores. Este modelo híbrido integra unidades recurrentes bidireccionales con gating (BiGRU), redes de memoria a largo corto plazo (LSTM) y un mecanismo de atención multi-cabeza (MHA) para capturar dependencias temporales bidireccionales, modelar patrones secuenciales y mejorar la representación de características contextuales. Los resultados experimentales en los conjuntos de datos de referencia CICIoMT2024 y EdgeIIoTset demuestran una robustez de dominio cruzado excepcional, logrando precisiones de detección del 99.13% y 99.34%, respectivamente. Además, BiGAT-ID exhibe una eficiencia en tiempo de ejecución notable, con tiempos de inferencia tan bajos como 0.0002 segundos por instancia en IoMT y 0.0001 segundos en escenarios IIoT, lo que lo hace adecuado para la detección de amenazas en tiempo real en entornos IoT heterogéneos.

La identificación de situaciones anómalas en sistemas de información y telecomunicaciones es fundamental, y Lebedev y Rzayev (2023) proponen un método basado en la segmentación de muestras de datos de tráfico de red para optimizar la precisión de clasificación. La hipótesis central es que las propiedades de los datos en las muestras, como el volumen o la frecuencia de mensajes, son tan influyentes como el propio algoritmo de clasificación para lograr indicadores cualitativos óptimos. El método busca utilizar algoritmos clasificadores que demuestren los mejores indicadores de calidad en segmentos de datos individuales, adaptándose a los cambios en las propiedades del tráfico que pueden ocurrir con el tiempo. La implementación implica un preprocesamiento de la información y la detección de puntos de cambio en las series temporales para dividir el flujo continuo de datos en segmentos homogéneos. Los experimentos realizados con el conjunto de datos NSL-KDD demostraron que la segmentación y la asignación de clasificadores óptimos a cada segmento pueden mejorar la calidad general del procesamiento de la muestra en aproximadamente un 5%.

Arabiat y Altayeb (2024) investigan la creciente preocupación por la ciberseguridad en el Internet de las Cosas (IoT) mediante la evaluación de clasificadores de Machine Learning (ML) y Deep Learning (DL) para la predicción de ataques. Su estudio propone un modelo de sistema de detección de intrusiones (IDS) que combina Random Forest (RF), Redes Neuronales Artificiales (ANN), Regresión Logística (LR) y Support Vector Machine (SVM) para detectar diversos tipos de ataques IoT, incluyendo ARP\_poisoning, DOS\_SYN\_Hping y NMAP\_FIN\_SCAN. Utilizando el conjunto de datos RT-IoT2022 y la herramienta de minería de datos Orange3, lograron resultados sobresalientes, con el modelo RF alcanzando una precisión de clasificación del 99.9% y el modelo ANN un 99.8%. La aplicación de validación cruzada de 10 pliegues y la reducción de datos mediante análisis discriminante lineal fueron cruciales para la alta precisión y para evitar el sobreajuste. Los autores sugieren que futuras investigaciones podrían verificar estos resultados con datos empíricos y explorar el aprendizaje distribuido/federado para sistemas basados en RF.

Para la detección de ataques de PortScan, Kareem et al. (2023) proponen un enfoque basado en Machine Learning utilizando los algoritmos JRip y OneR. Su investigación se enfoca en mejorar la precisión de detección mediante una estrategia de selección de características híbrida que combina el filtrado por varianza y la razón de ganancia de información (IGR). Al aplicar este método al conjunto de datos CICIDS2017, lograron distinguir eficazmente entre el tráfico normal y los ataques de PortScan, con el algoritmo JRip obteniendo una precisión destacada del 99.84%. Este estudio subraya la importancia de una selección de características minuciosa para construir modelos de clasificación eficientes y resalta cómo los algoritmos basados en reglas pueden ofrecer una alta interpretabilidad, lo cual es esencial en la seguridad de redes. Se sugiere que el trabajo futuro incluya la aplicación de la técnica en entornos prácticos como SDN e IoT, utilizando conjuntos de datos más recientes.

Al-Khazaali et al. (2025) realizan un estudio de caso sobre las características del tráfico de escaneo de puertos generado por Nmap para proporcionar información valiosa que permita desarrollar sistemas de detección de intrusiones (IDS) más efectivos. La investigación identifica varios "Indicadores de Escaneo" (IoS), incluyendo la distribución de puertos de origen y destino, medidas estadísticas y atributos relacionados con el tiempo, que pueden servir como características distintivas para detectar el tráfico de escaneo. Mediante el uso de Nmap y Wireshark en un entorno simulado, los autores demuestran cómo el comportamiento de Nmap en la selección de puertos es aleatorio por defecto, a diferencia de otras herramientas como Metasploit, que a menudo utiliza patrones ascendentes. Estas "huellas digitales" del comportamiento de escaneo son cruciales para que los analistas de ciberseguridad reconozcan no solo la presencia de un escaneo, sino también la herramienta específica utilizada, facilitando así respuestas más informadas y precisas.

En un esfuerzo por construir un sistema de protección de red más robusto, Guo et al. (2025) proponen una tecnología dinámica de seguridad anti-mapeo de red que utiliza Modelos Ocultos de Markov (HMM) y redes de Memoria Larga a Corto Plazo (LSTM) para combatir el escaneo ilegal. Su modelo Bi-LSTM+Attention es particularmente efectivo, logrando una precisión del 98% en el conjunto de datos UNSW-NB15 y reduciendo la tasa de falsas alarmas en un 30% en comparación con los modelos LSTM tradicionales. La investigación enfatiza la importancia de los mecanismos de defensa inteligentes y la capacidad de los modelos para adaptarse dinámicamente a entornos de red complejos y cambiantes. Este enfoque avanzado es capaz de aprender y adaptarse automáticamente a nuevos patrones de amenazas, lo que es crucial para mantener capacidades de detección eficientes en un panorama de seguridad en constante evolución. Aunque el modelo tiene altos requisitos de recursos computacionales, sus ventajas significativas en la mejora de la precisión de detección justifican su implementación, y se plantean optimizaciones futuras para reducir costos.

Jafarian et al. (2023) proponen un mecanismo de defensa innovador para proteger las redes empresariales contra ataques de escaneo de red internos y externos. El enfoque se basa en la premisa de que la comunicación legítima entre dos máquinas generalmente es precedida por una resolución DNS; por lo tanto, cualquier comunicación no precedida por una consulta DNS se marca como un escaneo. Para mejorar la efectividad de la detección, especialmente contra escáneres sigilosos y adaptativos, la investigación incorpora la manipulación de los valores TTL (Time-to-Live) de las respuestas DNS, lo que reduce la probabilidad de evasión al acortar la validez de los registros DNS en caché. Los experimentos en un entorno simulado a gran escala, utilizando conjuntos de datos de flujo de red del Laboratorio Nacional de Los Álamos, demostraron que esta manipulación de TTL puede ralentizar el éxito del escaneo hasta 20,000 veces, logrando una precisión superior al 96% para escaneos internos y más del 98% para escaneos externos. Además, el estudio introduce una técnica de escaneo adaptativo basada en caché DNS que evade métodos previos, pero muestra la efectividad del enfoque propuesto contra esta amenaza evolucionada.

--------------------------------------------------------------------------------

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 Sustainable Development, 29(1).

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.

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.

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(2), 207–220.

Jafarian, J. H., Abolfathi, M., & Rahimian, M. (2023). Detecting network scanning through monitoring and manipulation of DNS traffic. IEEE Access, 11, 20267–20283.

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.

Kushwaha, J. P., Bhadauria, S., & Tapaswi, S. (2025). Unveiling IoT ecosystem security: A review of intelligent IDS, trends, challenges, and future directions. Computers and Electrical Engineering, 128, 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.

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.

Shenfield, A., Day, D., & Ayesh, A. (2018). Intelligent intrusion detection systems using artificial neural networks. ICT Express, 4(2), 95–99.