REVISION SISTEMATICA METODOLOGIA PRISMA

Pregunta de Investigacion:

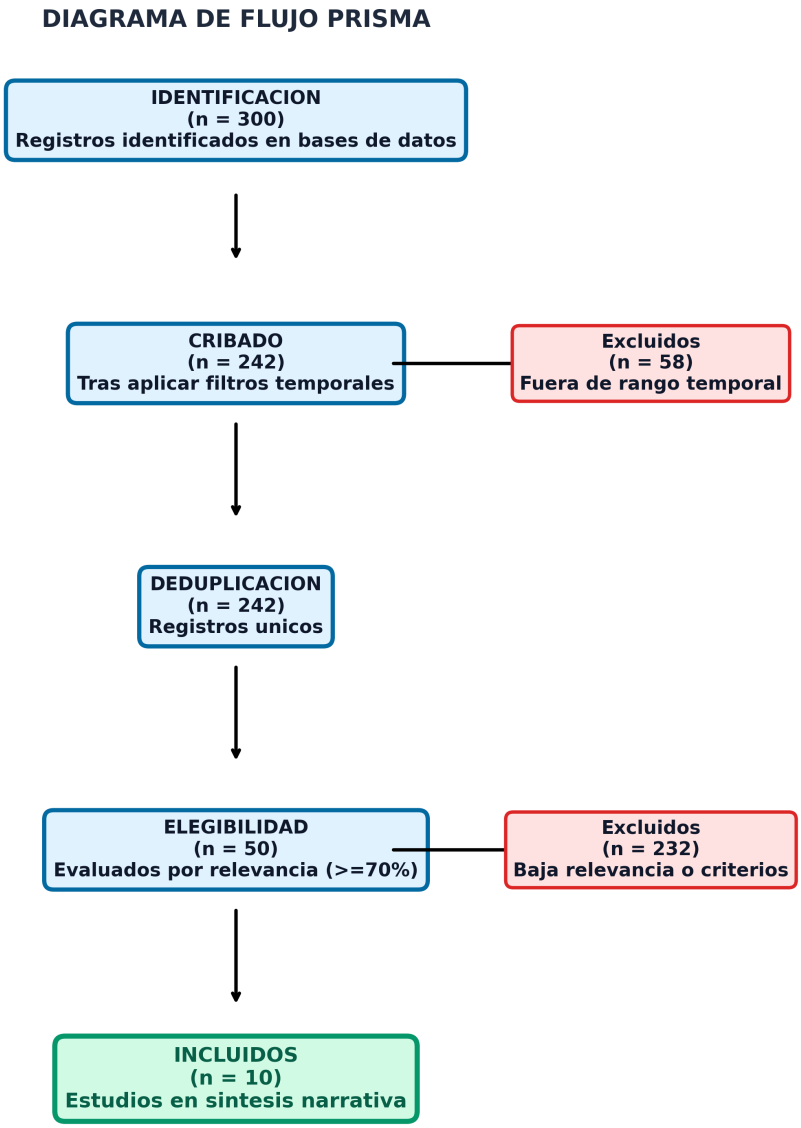
Cul es la eficacia de los modelos de Deep Learning en la deteccion de intrusiones en redes IoT?

10 Estudios Incluidos

Universidad Privada Antenor Orrego

Asistente de Revision Sistematica con IA

1. Diagrama de Flujo PRISMA



2. Sintesis Narrativa

Sntesis Narrativa

1. Introduccion

La creciente adopcion del Internet de las Cosas (IoT) ha trado consigo un aumento en las vulnerabilidades de seguridad, lo que ha llevado a la necesidad de desarrollar sistemas de deteccion de intrusiones (IDS) ms eficientes. Esta revision sistemtica examina la eficacia de los modelos de Deep Learning (DL) en la deteccion de intrusiones en redes IoT, basndose en diez estudios recientes. Los hallazgos indican que, aunque los modelos de DL muestran un rendimiento superior en comparacion con los enfoques tradicionales, existen desafos significativos en trminos de datos, interpretabilidad y adaptabilidad a diferentes entornos de IoT.

2. Eficacia de Algoritmos

Los estudios revisados presentan una variedad de enfoques de DL, destacando su eficacia en la deteccion de intrusiones. Por ejemplo, Wali et al. (2023) reportaron una precision del 99% en la deteccion de ataques en redes de flujo, mientras que Narayana et al. (2024) lograron una precision de hasta el 99.98% utilizando un modelo Bi-LSTM modificado. En contraste, Mahadevappa et al. (2021) encontraron que el Multi-Layer Perception (MLP) alcanzo solo un 79% de precision, lo que sugiere que no todos los algoritmos de ML son igualmente efectivos en entornos de IoT. Adems, el uso de tcnicas avanzadas como el Transfer Learning (Eva et al., 2022) y el uso de redes neuronales complejas (Engy et al., 2024) tambin demostraron ser efectivos, alcanzando precisiones superiores al 97%.

3. Limitaciones Metodologicas

A pesar de los resultados prometedores, varios estudios identifican limitaciones metodologicas. Por ejemplo, la dependencia de conjuntos de datos equilibrados y etiquetados es un desafo comn. Eva et al. (2022) sealaron que la escasez de datos etiquetados limita la eficacia de los modelos de DL en la deteccion de ataques de da cero. Adems, la falta de interpretabilidad de los modelos de DL fue un tema recurrente, con Demostenes et al. (2023) enfatizando la necesidad de mecanismos de seleccion de caractersticas explicables para mejorar la confianza en los sistemas de deteccion. Asimismo, el alto ndice de falsos positivos, como se menciona en el trabajo de Jamshidi et al. (2025), sigue siendo un obstculo crtico para la implementacion prctica de estos sistemas.

4. Metodologas Empleadas

Los estudios revisados emplean diversas metodologas, desde redes neuronales convolucionales (CNN) hasta arquitecturas de redes neuronales recurrentes (RNN). La mayora de los estudios utilizaron conjuntos de datos especficos de IoT, como ToN-IoT y CICIDS, para evaluar el rendimiento de sus modelos. Sin embargo, la calidad de la evidencia vara, ya que algunos estudios, como el de Mahadevappa et al. (2021), se basaron en conjuntos de datos ms antiguos como NSL-KDD, lo que puede no reflejar adecuadamente las amenazas actuales en entornos de IoT. Adems, la comparacion entre modelos a menudo carece de estandarizacion en las mtricas de evaluacion, lo que dificulta la generalizacion de los resultados.

5. Limitaciones y Gaps

Los estudios identifican varias limitaciones y reas no exploradas. La escasez de datos etiquetados y equilibrados es un problema crtico que limita la capacidad de los modelos de DL para generalizar en entornos del mundo real (Eva et al., 2022). Adems, la mayora de los estudios se centran en la deteccion de intrusiones, pero no abordan adecuadamente la

respuesta a incidentes o la adaptacion dinmica a nuevas amenazas (Jamshidi et al., 2025). Tambin se observa una falta de investigacion sobre la implementacion de estos modelos en dispositivos IoT con recursos limitados, lo que podra restringir su aplicabilidad en escenarios reales.

6. Conclusiones

En conclusion, los modelos de Deep Learning muestran un potencial significativo para mejorar la deteccion de intrusiones en redes IoT, con tasas de precision que superan el 99% en varios estudios. Sin embargo, las limitaciones en la disponibilidad de datos, la interpretabilidad de los modelos y la adaptabilidad a diferentes entornos de IoT representan desafos que deben abordarse para lograr una implementacion efectiva y confiable. La investigacion futura debera centrarse en la creacion de conjuntos de datos ms robustos, el desarrollo de modelos interpretables y la exploracion de estrategias de respuesta a incidentes para fortalecer la seguridad en el ecosistema IoT.

Referencias Bibliogrficas

1. Jamshidi, S., Nikanjam, A., Wazed, N.K., & Khomh, F. (2025). Leveraging Machine Learning Techniques in Intrusion Detection Systems for Internet of Things. arXiv Preprint. https://arxiv.org/pdf/2504.07220v1

2. Wali, K.N., S, A.M., A, K.M., Sultan, A., Naghmeh, M., Abdulwahab, A., Safi, U., Naila, N., & Jawad, A. (2023). A hybrid deep learning-based intrusion detection system for IoT networks. Mathematical biosciences and engineering : MBE, 20(8), 13491-13520. https://doi.org/10.3934/mbe.2023602

3. Eva, R., Pol, V., Beatriz, O., Jos, C.J., Javier, V., Alejandro, P.M., & Ramon, C. (2022). Transfer-Learning-Based Intrusion Detection Framework in IoT Networks. Sensors (Basel, Switzerland), 22(15). https://doi.org/10.3390/s22155621

4. Mahadevappa, P., Muzammal, S.M., & Murugesan, R.K. (2021). A Comparative Analysis of Machine Learning Algorithms for Intrusion Detection in Edge-Enabled IoT Networks. arXiv Preprint. https://arxiv.org/pdf/2111.01383v1

5. Mousa, A. & Sung-Chul, H. (2023). An Adaptive Intrusion Detection System in the Internet of Medical Things Using Fuzzy-Based Learning. Sensors (Basel, Switzerland), 23(22). https://doi.org/10.3390/s23229247

6. Narayana, C.S.S., Prakash, S.S., Jaroslav, F., Parameshachari, B.D., Lakshmi, S.V., & Przemyslaw, F. (2024). OOA-modified Bi-LSTM network: An effective intrusion detection framework for IoT systems. Heliyon, 10(8), e29410. https://doi.org/10.1016/j.heliyon.2024.e29410

7. Engy, E., M, E.W., Haitham, E., Maazen, A., I, I.M., & Farouk, E.G. (2024). Deep Complex Gated Recurrent Networks-Based IoT Network Intrusion Detection Systems. Sensors (Basel, Switzerland), 24(18). https://doi.org/10.3390/s24185933

8. Demostenes, Z.R., Ogobuchi, D.O., Sarah, M.S., Ekikere, U.U., & Henrique, K.J. (2023). Attentive transformer deep learning algorithm for intrusion detection on IoT systems using automatic Xplainable feature selection. PloS one, 18(10), e0286652. https://doi.org/10.1371/journal.pone.0286652

9. B, S.S.K., Prasanna, M., V, M., Prabhu, J., M, S.K., & Muhammad, A.S. (2022). Design and Analysis of Multilayered Neural Network-Based Intrusion Detection System in the Internet of Things Network. Computational intelligence and neuroscience, 2022, 9423395. https://doi.org/10.1155/2022/9423395

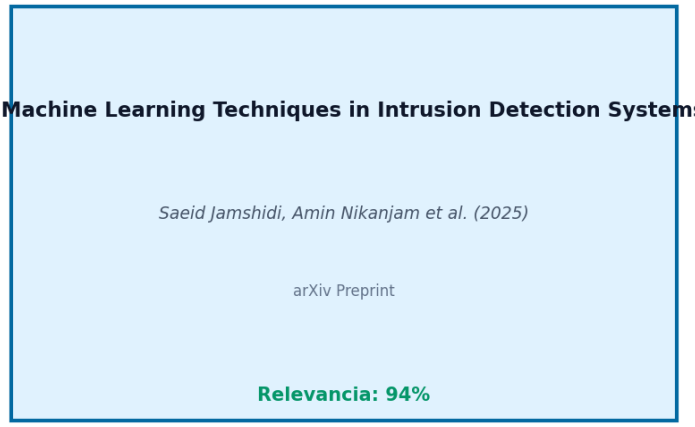
10. Khalid, A., A, S.A., T, S.F., & K, A.R. (2021). IoT Intrusion Detection Taxonomy, Reference Architecture, and Analyses. Sensors (Basel, Switzerland), 21(19). https://doi.org/10.3390/s21196432

3. Articulos Destacados

Articulo 1 (Relevancia: 94.2%)

Leveraging Machine Learning Techniques in Intrusion Detection Systems for Internet of Things

Saeid



Articulo 2 (Relevancia: 94.0%)

A hybrid deep learning-based intrusion detection system for IoT networks.

Khan,