|  |  |
| --- | --- |
|  | **Referencia universidad** |
|  | **Referencias externas** |

**TABLA DE APORTES Y VACÍOS**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **No.** | **TÍTULO** | **AUTOR** | **APORTE** | **VACÍO** | **Resumen** |
|  | Título del documento | Autor del documento | Que sirve para mi proyecto | En que se diferencia de mi proyecto | Terminado |
| **1** | **Detection and prediction of DDoS cyber attacks using spline functions**  **https://ieeexplore-ieee-org.bdigital.udistrital.edu.co/document/9766940** | **Serhii Kivalov; Irina Strelkovskaya** | **Un ejemplo de predicción de ataques DDoS utilizando funciones spline** | **No es específicamente para redes IOT, No es con DL, aunque las splines si son funciones de activación en Modelos de DL** |  |
| **2** | **Cyber AI: Real defense**  **https://www2.deloitte.com/us/en/insights/focus/tech-trends/2022/future-of-cybersecurity-and-ai.html** |  | **Un análisis de la importancia de la utilización de inteligencia artificial y modelos para el la prevención de ataques de ciberseguridad** | **No es tesis** |  |
| **3** | **Investigation of Machine Learning Techniques in Intrusion Detection System for IoT Network**  **https://ieeexplore-ieee-org.bdigital.udistrital.edu.co/document/9315900/references#references** | **S. Shinly Swarna Sugi; S. Raja Ratna** | **Predicción de ataques mediante ML específicamente a redes IOT** | **Solo ML** |  |
| **4** | **Detección de amenazas en Redes IoT empleando modelo híbrido de Machine Learning y Deep Learning** | Elina Valentina Jaimes Bastidas | **Utiliza un modelo hibrido de ML Y DL** |  | **X** |
| **5** | MODELO DE DETECCIÓN DE ATAQUES DDOS (DISTRIBUTED DENIAL OF SERVICES), CON BASE EN EL CLASIFICADOR DECISION TREE  https://repository.udistrital.edu.co/bitstream/handle/11349/30117/CarvajalHoyosCamiloAndres2022.pdf?sequence=1&isAllowed=y | JUAN SEBASTIAN SUSA VELANDIA CAMILO ANDRÉS CARVAJAL HOYOS | **Predicción de ataques mediante dos métodos, decisión tree** | **No es especificamente redes IOT, Esto es ML** | **X** |
| **6** | Sistema preventivo contra ataques de denegación de servicio web utilizando Deep Learning  https://repositorio.itm.edu.co/bitstream/handle/20.500.12622/4674/JuanCanola\_2021.pdf?sequence=1 | Juan Fernando Cañola García | **Predicción de ataques con DL** | **No es especificamente redes IOT no utiliza redes convolucionales** |  |
| **7** | Propuesta de detección y mitigación de ataques dedenegación de servicios en las redes institucionales DGI  https://core.ac.uk/download/pdf/336876952.pdf | Ing. Wilfredo Rodríguez Aburto  Ing. Pedro José Castellón Mena | **Sistema para detección de ataques DOS** | **No utiliza IA y no es en redes IOT** |  |
| **8** | Una revisión del aprendizaje profundo aplicado a la ciberseguridad  https://incyt.upse.edu.ec/ciencia/revistas/index.php/rctu/article/view/671/539 | Daniel Quirumbay yagual  Carlos Andres Castillo  Ivan Alberto  Coronel | **Revisa cuatro Algoritmos de DL**  **MLP**  **CNN**  **RNN**  **LSTM**  **DTL** |  |  |
| **9** | Analysis of Anomaly Detection and Identification Methods in 5G Traffic  https://ieeexplore-ieee-org.bdigital.udistrital.edu.co/document/9660920 |  |  |  |  |
| **10** | T´ecnicas de Inteligencia Artificial para Sistemas de Detecci´on de Intrusiones  https://repositorio.uci.cu/jspui/bitstream/123456789/9679/1/UCIENCIA\_2021\_paper\_224.pdf | Ing. Darvis Dorvigny Dorvigny1\*, Esp. Dennis Barrera P´erez2 , Lic. Lester Rodr´ıguez Vallejo3 |  |  |  |
| **11** | Clasificación de Ataques a una Red de Telecomunicación con Deep Learning  https://biblus.us.es/bibing/proyectos/abreproy/71954/fichero/TFM-1954+TRAPERO+ESTEPA%2C+MAR%C3%8DA+DOLORES.pdf | Autora: María Dolores Trapero Estepa |  |  |  |
| **12** | Las amenazas de seguridad a las que se enfrenta IoT y las soluciones en desarrollo [ ] | Dennis Rolando David Patiño, Estudiante Especialización en Telecomunicaciones Móviles, UDFJCEdgar Alexander Sánchez Galindo, Estudiante Especialización en Telecomunicaciones Móviles, UDFJC |  |  | **x** |
| **13** | Mecanismos de seguridad en el internet de las cosas  https://revistas.udistrital.edu.co/index.php/vinculos/article/view/15758 | Andrés Camilo Morales-Suárez , Shayther Stewar Díaz-Ávila , Miguel Ángel Leguizamón-Páez |  |  | **X** |
| **14** | Un método para la identificación y  prevención temprana de incidentes  de ciberseguridad en dispositivos  del Internet de las Cosas  https://repositorio.unal.edu.co/handle/unal/81148 | Jhon Alexander Parra Jiménez |  |  | **X** |
| **15** | Diseño de un modelo de detección de intrusos en entornos IoT usando inteligencia artific https://repository.udistrital.edu.co/handle/11349/29671ial. |  |  |  | **X** |
| **16** | Defensa contra intrusos en redes de dispositivos IoT usando técnicas de Blockchain y Machine Learning  https://repositorio.uniandes.edu.co/handle/1992/48617 |  |  |  | **7X** |
| **17** |  |  |  |  |  |
| **18** |  |  |  |  |  |
| **19** |  |  |  |  |  |
| **20** |  |  |  |  |  |