II SICDAS 2021, LIMA-PERU

SEGURIDAD CIBERNÉTICA
Prevención de Fraudes & Redes Neuronales Artificiales

Moises Mescua Salhuana,[1] *PhD, MBA. P.Eng.*
moises.mescua@mesol.ca

(1) Consultor senior de TI en organizaciones del Perú y Norte América, docente externo/investigador en ciencia de datos e inteligencia artificial en la UNMSM.

RESUMEN

La digitalización impacta cada vez más en todos los aspectos de nuestras vidas e industrias. Somos testigos del crecimiento de la demanda de dispositivos electrónicos, redes, infraestructura en la nube, sistemas informáticos, aplicaciones de Inteligencia Artificial y Big Data Analytics para contribuir una mejor gestión de los datos en las organizaciones.
La interoperabilidad de los sistemas e integración de los dispositivos electrónicos incrementa la vulnerabilidad en la seguridad de la información, y puede ser blanco de ataques cibernéticos que están generando billones de dólares en perdidas a las organizaciones y agencias de gobierno alrededor del mundo [1]. La implementación de medidas efectivas de ciberseguridad es particularmente desafiante hoy en día porque hay más dispositivos que personas y los atacantes son cada vez más innovadores. La reciente vulnerabilidad que está generando el 'Log4j' de Apache Software en las aplicaciones, revelado el 24 noviembre del 2021 por un ingeniero de seguridad de la compañía Alibaba Cloud, ha puesto en jaque a miles de organizaciones y gobiernos en ser blancos de ataques cibernéticos [2].
La aplicación de algoritmos de aprendizaje profundo, particularmente las redes neuronales artificiales (ANN), RNN, CNN, GAN, etc. son necesarias para incrementar los niveles de seguridad de nuestras aplicaciones y dispositivos electrónicos [3][4]. En consecuencia, hoy en día una efectiva y rápida detección de un intruso en nuestras redes y sistemas informáticos solo será posible empleando la inteligencia artificial.

Palabras claves: Seguridad cibernética, Redes Neuronales Artificiales, detección

Referencias

[1] Canadian Centre for Cyber Security, Canada, "Cyber Centre Expertise", 2021, https://cyber.gc.ca/en/

[2] Cybersecurity & Infrastructure Security Agency, United States, "Alert (AA21-356A), Mitigating Log4Shell and Other Log4j-Related Vulnerabilities", December 23, 2021, https://cisa.gov/uscert/ncas/alerts/aa21-356a.

[3] Matt R. Cole, “Deep Learning” with C#, .NET and Kelp.Net, 2019, pp. 5-62, BPB Publication, India.
[4] Oliver Durr, Beate Sick with Elvis Murina, “Probabilistic Deep Learning,” with Python, Keras, and TensorFlow, 2020, Manning Publication Co. Shelter Island, NY 11964.

CYBER SECURITY
Fraud Prevention & Artificial Neural Network (ANN)

ABSTRACT

Digitization increasingly impacts all aspects of our lives and industries. We are witnessing the growth in demand for electronic devices, networks, cloud infrastructure, computer systems, Artificial Intelligence applications and Big Data Analytics to contribute to better data management in organizations. The interoperability of systems and integration of electronic devices increases vulnerability in information security, and can be the target of cyber-attacks that are generating billions of dollars in losses to organizations and government agencies around the world [1]. Implementing effective cybersecurity measures is particularly challenging today because there are more devices than people and attackers are increasingly innovative. The recent vulnerability that Apache Software's 'Log4j' is generating in applications, revealed on November 24, 2021 by a security engineer from the Alibaba Cloud company, has put thousands of organizations and governments in check in being targets of cyber-attacks [2].The application of deep learning algorithms, particularly artificial neural networks (ANN), RNN, CNN, GAN, etc. are necessary to increase the security levels of our applications and electronic devices [3][4]. Consequently, today an effective and rapid detection of an intruder in our networks and computer systems will only be possible using artificial intelligence.

Keywords: Cybersecurity, Artificial Neural Networks, detection