World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:15, No:07, 2021

Deep Learning and Accurate Performance Measure Processes for Cyber Attack Detection among Web Logs

Authors : Noureddine Mohtaram, Jeremy Patrix, Jerome Verny

Abstract : As an enormous number of online services have been developed into web applications, security problems based on web applications are becoming more serious now. Most intrusion detection systems rely on each request to find the cyber-attack rather than on user behavior, and these systems can only protect web applications against known vulnerabilities rather than certain zero-day attacks. In order to detect new attacks, we analyze the HTTP protocols of web servers to divide them into two categories: normal attacks and malicious attacks. On the other hand, the quality of the results obtained by deep learning (DL) in various areas of big data has given an important motivation to apply it to cybersecurity. Deep learning for attack detection in cybersecurity has the potential to be a robust tool from small transformations to new attacks due to its capability to extract more high-level features. This research aims to take a new approach, deep learning to cybersecurity, to classify these two categories to eliminate attacks and protect web servers of the defense sector which encounters different web traffic compared to other sectors (such as e-commerce, web app, etc.). The result shows that by using a machine learning method, a higher accuracy rate, and a lower false alarm detection rate can be achieved.

Keywords : anomaly detection, HTTP protocol, logs, cyber attack, deep learning
Conference Title : ICICA 2021 : International Conference on Industrial Cybersecurity and Applications
Conference Location : Rome, Italy
Conference Dates : July 22-23, 2021