

Machine Learning based Intrusion Detection System for Web-Based Attacks

Submitted by grigby1 on Tue, 04/27/2021 - 2:38pm

Title Machine Learning based Intrusion Detection System for Web-Based Attacks
Publication Type Conference Paper
Year of Publication 2020
Authors [Sharma, S.](#), [Zavarsky, P.](#), [Butakov, S.](#)
Conference Name 2020 IEEE 6th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS)
Date Published May 2020
Publisher IEEE
ISBN Number 978-1-7281-6873-9
Keywords [Big Data](#), [detection](#), [feature extraction](#), [machine learning](#), [Metrics](#), [pubcrawl](#), [resilience](#), [Resiliency](#), [Scalability](#), [security](#), [web-based attacks](#)

Abstract Various studies have been performed to explore the feasibility of detection of web-based attacks by machine learning techniques. False-positive and false-negative results have been reported as a major issue to be addressed to make machine learning-based detection and prevention of web-based attacks reliable and trustworthy. In our research, we tried to identify and address the root cause of the false-positive and false-negative results. In our experiment, we used the CSIC 2010 HTTP dataset, which contains the generated traffic targeted to an e-commerce web application. Our experimental results demonstrate that applying the proposed fine-tuned feature set extraction results in improved detection and classification of web-based attacks for all tested machine learning algorithms. The performance of the machine learning algorithm in the detection of attacks was evaluated by the Precision, Recall, Accuracy, and F-measure metrics. Among three tested algorithms, the J48 decision tree algorithm provided the highest True Positive rate, Precision, and Recall.

URL <https://ieeexplore.ieee.org/document/9123026>
DOI [10.1109/BigDataSecurity-HPSC-IDS49724.2020.00048](https://doi.org/10.1109/BigDataSecurity-HPSC-IDS49724.2020.00048)

Citation Key sharma_machine_2020



[Big Data](#) [detection](#) [feature extraction](#) [machine learning](#) [Metrics](#) [pubcrawl](#) [resilience](#) [Resiliency](#) [Scalability](#) [security](#) [web-based attacks](#)
