Adaptive machine learning-based alarm reduction via edge computing for distributed intrusion detection systems - DTU Orbit (24/05/2019)

Adaptive machine learning-based alarm reduction via edge computing for distributed intrusion detection systems: Adaptive Machine Learning-based Distributed IDS Alarm Reduction via Edge Computing

To protect assets and resources from being hacked, intrusion detection systems are widely implemented in organizations around the world. However, false alarms are one challenging issue for such systems, which would significantly degrade the effectiveness of detection and greatly increase the burden of analysis. To solve this problem, building an intelligent false alarm filter using machine learning classifiers is considered as one promising solution, where an appropriate algorithm can be selected in an adaptive way in order to maintain the filtration accuracy. By means of cloud computing, the task of adaptive algorithm selection can be offloaded to the cloud, whereas it could cause communication delay and increase additional burden. In this work, motivated by the advent of edge computing, we propose a framework to improve the intelligent false alarm reduction for DIDS based on edge computing devices. Our framework can provide energy efficiency as the data can be processed at the edge for shorter response time. The evaluation results demonstrate that our framework can help reduce the workload for the central server and the delay as compared to the similar studies.

General information
Publication status: Accepted/In press
Organisations: Department of Applied Mathematics and Computer Science, Cyber Security, Guangzhou University, University of Luxembourg, Technical University of Denmark
Contributors: Wang, Y., Meng, W., Li, W., Liu, Z., Liu, Y., Xue, H.
Number of pages: 12
Publication date: 2019
Peer-reviewed: Yes

Publication information
Journal: Concurrency and Computation: Practice & Experience
Article number: e5101
ISSN (Print): 1532-0626
Ratings:
BFI (2019): BFI-level 2
Web of Science (2019): Indexed yes
Original language: English
Keywords: Distributed system, Edge computing, Intelligent false alarm filter, Intrusion detection, Machine learning
DOIs: 10.1002/cpe.5101
Source: Findit
Source-ID: 2443008338
Research output: Contribution to journal › Journal article – Annual report year: 2019 › Research › peer-review