Open Science Index, Computer and Systems Engineering Vol:17, No:04, 2023 publications.waset.org/abstracts/162951.pdf

Anomaly Detection Based on System Log Data

Authors : M. Kamel, A. Hoayek, M. Batton-Hubert

Abstract : With the increase of network virtualization and the disparity of vendors, the continuous monitoring and detection of anomalies cannot rely on static rules. An advanced analytical methodology is needed to discriminate between ordinary events and unusual anomalies. In this paper, we focus on log data (textual data), which is a crucial source of information for network performance. Then, we introduce an algorithm used as a pipeline to help with the pretreatment of such data, group it into patterns, and dynamically label each pattern as an anomaly or not. Such tools will provide users and experts with continuous real-time logs monitoring capability to detect anomalies and failures in the underlying system that can affect performance. An application of real-world data illustrates the algorithm.

Keywords : logs, anomaly detection, ML, scoring, NLP
Conference Title : ICLDQAD 2023 : International Conference on Linked Data Quality and Anomaly Detection
Conference Location : Athens, Greece
Conference Dates : April 03-04, 2023