IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 7, April 2023

Multi Perspective Robust Deep Analysis Cyber Anomaly Detection on HDFS Log using Transformers

Yogaraja G S R[1], Deepak M[2], Gowtham K A[3], Kiran S[4], Laxmipathi R[5]
Assistant Professor, Department of Information Science and Engineering[1]
Students, Department of Information Science and Engineering[2,3,4,5]
S J C Institute of Technology, Chickballapur, India

Abstract: *Log analysis is one of the main techniques engineers use to troubleshoot faults of large- scale software systems. During the past decades, many log analysis approaches have been proposed to detect system anomalies reflected by logs. They usually take log event counts or sequential log events as inputs and utilize machine learning algorithms including deep learning models to detect system anomalies. These anomalies are often identified as violations of quantitative relational patterns or sequential patterns of log events in log sequences. While these systems provide users rich services, they also bring new security and reliability challenges. One of the challenges is locating system faults and discovering potential issues. While anomaly detection has been widely studied in the context of network data, operational data presents several new challenges, including the volatility and sparseness of data, and the need to perform fast detection (complicating application of schemes that require offline processing or large/stable data sets to converge). This paper proposes a log sequence anomaly detection method based on neural network training and feature extraction. This method uses BERT (Bidirectional Encoder Representations from Transformers) to extract the semantic features and statistical features of the log sequence.*

Keywords: HDFS

REFERENCES

[1]. M. Kezunovic, P. Pinson, Z. Obradovic, S. Grijalva, T. Hong, and R. J. Bessa, ‘‘Big data analytics for future electricity grids, ’’Electr. Power Syst. Res., vol. 189, p. 106788, Dec. 2020.
[2]. L. Wei, W. Guo, F. Wen, G. Ledwich, Z. Liao, and J. Xin, ‘‘An online intelligent alarm- processing system for digital substations, ’’IEEE Trans. Power Del., vol. 26, no. 3, pp. 1615– 1624, Jul. 2011.
[3]. S. Pandey, A. K. Srivastava, and B. G. Amidan, ‘‘A real time event detection, classification and localization using synchro phasor data, ’’IEEE Trans. Power Syst., vol. 35, no. 6, pp. 4421–4431, Nov. 2020.
[4]. N. Baranovic, P. Andersson, I. Ivankovic, K. Zubrinic-Kostovic, D. Peharda, and J. E. Larsson, ‘‘Experiences from intelligent alarm processing and decision support tools in smart grid transmission control centers, ’’in Proc. CIGRE Session, Paris, France, Aug. 2016, pp. 1–10.
[5]. C. Feng, L. Wang, R. Ye, J. Gu, L. Xie, Y. Wang, Q. Feng, and C. Cui, ‘‘Research and application of alarm optimization mechanism in power grid operation monitoring, ’’in Proc. IEEE 5th Adv. Inf. Technol., Electron. Autom. Control Conf. (IAEAC), Chongqing, China, Mar. 2021, pp. 2352–2356.
[6]. D. B. Tesch, D. C. Yu, L.-M. Fu, and K. Vairavan, ‘‘A knowledge-based alarm processor for an energy management system, ’’IEEE Trans. Power Syst., vol. 5, no. 1, pp. 268–275, Feb. 1990.
[7]. G. Sun, X. Ding, Z. Wei, P. Shen, Y. Zhao, Q. Huang, L. Zhang, and H. Zang, ‘‘Intelligent classification method for grid-monitoring alarm messages based on information theory, ’’ Energies, vol. 12, no. 14, p. 2814, Jul. 2019.
[8]. D. S. Kirschen and B. F. Wollenberg, ‘‘Intelligent alarm processing in power systems, ’’Proc. IEEE, vol. 80, no. 5, pp. 663– 672, May 1992.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 7, April 2023