

Chapter 8

Machine Learning Applications for Anomaly Detection

Teguh Wahyono

Satya Wacana Christian University, Indonesia

Yaya Heryadi

Bina Nusantara University, Indonesia

ABSTRACT

The aim of this chapter is to describe and analyze the application of machine learning for anomaly detection. The study regarding the anomaly detection is a very important thing. The various phenomena often occur related to the anomaly study, such as the occurrence of an extreme climate change, the intrusion detection for the network security, the fraud detection for e-banking, the diagnosis for engines fault, the spacecraft anomaly detection, the vessel track, and the airline safety. This chapter is an attempt to provide a structured and a broad overview of extensive research on anomaly detection techniques spanning multiple research areas and application domains. Quantitative analysis meta-approach is used to see the development of the research concerned with those matters. The learning is done on the method side, the techniques utilized, the application development, the technology utilized, and the research trend, which is developed.

INTRODUCTION

The aim of this chapter is to describe several applications of machine learning for anomaly detection. Although has received considerable attention from many researchers since 90's, the anomaly detection problem remained an interesting problem in computer vision field. Its wide potential applications ranging from climate change, computer network intrusion detection, financial transaction fraud detection, engines fault detection, spacecraft anomaly detection to vessel track and the airline safety detection. The emerging applications of machine learning methods in the past ten years has received great interests from many researchers to adopt machine learning to address anomaly detection.

DOI: 10.4018/978-1-6684-6291-1.ch008

This paper started with literature review using quantitative analysis meta approach to analyze the main research progress, opportunities and trends, and research applications in the anomaly detection field. This systematic literature review will identify the most significant journals in the anomaly detection field, the opportunities and trends for anomaly detection method, identify research applications and trends in anomaly detection system and give the proposed method improvements for anomaly detection in the future.

This chapter is an attempt to provide a structured and a broad overview of extensive research on anomaly detection techniques spanning multiple research areas and application domains. quantitative analysis meta approach to see the development of the research concerned with those matters. The learning is done both on the method side, the techniques utilized, the application development, the technology utilized and the research trend which is developed.

BACKGROUND

Anomaly, also known as outliers, is a term refers to irregularity or deviation from the normal pattern (Chandola, et al., 2007). Yang (2007) referred the term anomaly to observation data that strongly inconsistent with the previous compiled data. Recently, Bloomquist (2015) defined anomaly as “*patterns or data points that do not conform to a well defined notion of normal behaviour.*”

Anomaly detection problem refers to the task of finding patterns in data that do not conform to expected behavior (Chandola, 2007). The problem is an interesting computer vision problem with many potential applications ranging from climate change detection, anomaly detection of fault tolerant robotic system (Jakimovski, 2011) to fraud transaction detection. In the past decade, anomaly detection problem has raised wide attention from various research domains due to its potential applications for recognizing indication that the underlying process that induces the data does not happen as expected. Depending on the context of the data, the detected anomalous data can be interpreted as either extreme climate change (Kawale, 2011), network security intrusion (Tsai, et al., 2010), medical diagnosis (Park, et al., 2015), engines fault (Djurđjanovic, et al., 2007), spacecraft anomaly detection (Fujimaki, et al., 2007), Mobility-Based Anomaly Detection in Cellular Mobile (Sun, et al., 2006) or vessel track and the airline safety diagnosis (Budalakoti et al., 2009).

Despite many studies have been reported, anomaly detection remained a challenging problem. A prominent study reported by (Chandola, et al., 2007) summarized several challenges in detecting anomaly as follows.

1. Defining a normal region which encompasses every possible normal behavior is very difficult. In addition, the boundary between normal and anomalous behavior is often not precise. Thus an anomalous observation which lies close to the boundary can actually be normal, and vice-versa.
2. When anomalies are the result of malicious actions, the malicious adversaries often adapt themselves to make the anomalous observations appear like normal, thereby making the task of defining normal behavior more difficult.
3. In many domains normal behavior keeps evolving and a current notion of normal behavior might not be sufficiently representative in the future. In medical research domain, concluded that the general pattern to be used as the expected behavior or reference is often unavailable.

28 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:

www.igi-global.com/chapter/machine-learning-applications-for-anomaly-detection/307449

Related Content

Automobile Predictive Maintenance Using Deep Learning

Sanjit Kumar Dash, Satyam Raj, Rahul Agarwal and Jibitesh Mishra (2021). *International Journal of Artificial Intelligence and Machine Learning* (pp. 1-12).

www.irma-international.org/article/automobile-predictive-maintenance-using-deep-learning/279274

Survey of Recent Applications of Artificial Intelligence for Detection and Analysis of COVID-19 and Other Infectious Diseases

Richard S. Segall and Vidhya Sankarasubbu (2022). *International Journal of Artificial Intelligence and Machine Learning* (pp. 1-30).

www.irma-international.org/article/survey-of-recent-applications-of-artificial-intelligence-for-detection-and-analysis-of-covid-19-and-other-infectious-diseases/313574

Three-Layer Stacked Generalization Architecture With Simulated Annealing for Optimum Results in Data Mining

K. T. Sanvitha Kasthuriarachchi and Sidath R. Liyanage (2021). *International Journal of Artificial Intelligence and Machine Learning* (pp. 1-27).

www.irma-international.org/article/three-layer-stacked-generalization-architecture-with-simulated-annealing-for-optimum-results-in-data-mining/279277

Image Fusion Techniques for Different Multimodality Medical Images Based on Various Conventional and Hybrid Algorithms for Disease Analysis

Rajalingam B., Priya R., Bhavani R. and Santhoshkumar R. (2020). *Applications of Advanced Machine Intelligence in Computer Vision and Object Recognition: Emerging Research and Opportunities* (pp. 159-196).

www.irma-international.org/chapter/image-fusion-techniques-for-different-multimodality-medical-images-based-on-various-conventional-and-hybrid-algorithms-for-disease-analysis/252627

Classification of Traffic Events in Mexico City Using Machine Learning and Volunteered Geographic Information

Magdalena Saldana-Perez, Miguel Torres-Ruiz and Marco Moreno-Ibarra (2022). *Research Anthology on Machine Learning Techniques, Methods, and Applications* (pp. 1107-1127).

www.irma-international.org/chapter/classification-of-traffic-events-in-mexico-city-using-machine-learning-and-volunteered-geographic-information/307501