Chapter 3

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.

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) refered 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 (Djurdjanovic, et al., 2007), spacecraft anomaly detection (Fujimaki, et al.,