Chapter 4
A Comparative Analysis of a Novel Anomaly Detection Algorithm with Neural Networks

Srijan Das
National Institute of Technology, India

Saurav Sharma
National Institute of Technology, India

Arpita Dutta
National Institute of TechnologyIndia

Sangharatna Godboley
National Institute of Technology, India

ABSTRACT

Anomaly Detection is an important research domain of Pattern Recognition due to its effects of classification and clustering problems. In this paper, an anomaly detection algorithm is proposed using different primitive cost functions such as Normal Perceptron, Relaxation Criterion, Mean Square Error (MSE) and Ho-Kashyap. These criterion functions are minimized to locate the decision boundary in the data space so as to classify the normal data objects and the anomalous data objects. The authors proposed algorithm uses the concept of supervised classification, though it is very different from solving normal supervised classification problems. This proposed algorithm using different criterion functions has been compared with the accuracy of the Neural Networks (NN) in order to bring out a comparative analysis between them and discuss some advantages.

1. INTRODUCTION

Anomalous objects are those odd ones out data objects that behave differently from most of the other objects in the system. The objective of anomaly detection is to find objects which are different from most of the other objects in the dataset. Often anomalous objects are known as outliers, since on a scatter plot of the data, they lie far away from other data points.Some causes of an outlier include poor data quality in the process of feature extraction, a measurement may be recorded incorrectly because of human error or the presence of noise and sometimes exceptionally good extracted data also deviates from the normally distributed data objects.

DOI: 10.4018/978-1-7998-0414-7.ch004

The categories of anomaly include point anomalies, contextual anomalies and collective anomalies. Point anomalies are those objects, if it is anomalous to the rest of the data. Contextual Anomalies are those data objects, if it is anomalous in a specific context but not otherwise. In such a case certain attributes are used to determine the context for that object. Collective anomalies are the collection of related data objects with respect to the data. Individually, these objects may not be an outlier, but collectively are anomalous (Chandola et al., 2009).

The labels associated with data instances denote whether that instance is normal data or anomalies. The operation of anomaly detection can be done in one of the following three modes: supervised anomaly detection, semi supervised anomaly detection, and unsupervised anomaly detection.

The anomaly detection problem is viewed as a special type of classification problem which is different from general supervised classification problems.This is because a supervised classification problem consists of a large number of positive and negative data points, whereas in anomaly detection the number of positive examples, that is the anomalies are very few in number (less than 2% of the total data samples). Due to such imbalanced composition of the dataset in anomaly detection, the decision boundary obtained is deviated and cannot correctly classify all the data points with accuracy. Hence, supervised classification cannot be used in such problems to classify the anomalies.

In this paper, the focus is on a comparative study of an anomaly detection algorithm using different gradient descent techniques with anomaly detection using neural networks. The output of the proposed algorithm is compared with the output of the Neural Networks. Here, different perceptron criteria are used in order to bring out a comparative study along with choosing a different learning rate used in the gradient descent methods.The rest of the article is organized as follows: Section 2 presents the related works. Section 3 dealswith basic concepts. Section 4 discusses our proposed approach. Section 5 deals with the detail experimental study, which also consists of Accuracy analysis and experimental metrics. Section 6 concludes our proposed approach and suggesting some future work.

2. RELATED WORKS

Barnett et al. (1994) described the definition of anomaly detection as the exceptional data objects that deviate from the characteristics of most of the data objects in the system. Aggarwal et al. (2001), notes outliers as noises lying outside a set of clusters. Thus, they concluded anomalies as noises introduced during data acquisition, which results in their aberrant behaviour along with their location which is outside from almost all defined clusters in the system.

Chandola et al. (2009) discussed many anomaly detection techniques that have been developed for certain application domains, while others are more generic. They have presented a survey report based upon the existing methods used for Anomaly Detection. This paper provides and structural and comprehensive overview of the existing anomaly detection methodologies. It also deals with different detection techniques with their complexities that helps to analyze which type of anomaly detection algorithm is suitable for a particular selected scenario.

The authors of (Bolton & Hand, 1999), (Ramaswamy et al., 2000) (Eskin et al., 2002), (Anguilli & Pizzuti, 2002), and (Zhang & Wang, 2006) describes statistical approaches where the earliest algorithms were used for anomaly detection have been discussed. These approaches encourage building a statistical model based on some assumed hypothesis. These models are obtained by training them with the available data objects which is further used on the test data objects to detect the deviated data objects