# EC2 CPU Utilization Outlier Detection Experiment

Research carried out by Liam Reid as part of Final Year Project and Dissertation: ‘Proposing new methods of detecting outliers in cloud resource data’.

## Abstract

Experiment success

## Introduction

**Background Information**

This document contains details of experiments carried out on cloud CPU utilization data and detecting outliers using newly implemented outlier detection techniques.

The data being analyzed is Amazon Elastic Compute Cloud (EC2) CPU usage. EC2 is a service provided by Amazon used for on-demand cloud infrastructure. Customers use the platform for its compute power, running multiple different kinds of operating systems for various applications [1].

Amazon Web Services (AWS) provides many tools for analyzing the metrics of an EC2 instance. CPU Utilization is arguably the most important metric, since it “identifies the processing power required run an application on a selected instance [2]”. Problems with an EC2 instance, or an application running on one, can often be identified by a discrepancy in CPU usage [3].

This CPU utilization data is labelled, meaning the outlier detection technique applied to the data can be evaluated based on accuracy, precision, recall and f1 score [4].

Graphical user interface

Description automatically generated with low confidence

Equation: Calculating F1 score [5].

**How is the experiment carried out?**

This experiment is carried using a webapp developed using dash. The purpose of this application is to apply outlier detection algorithms to datasets defined by the user. The application plots the data and generates scores for the chosen method. Accuracy, precision, recall and an f1 score will be calculated and displayed to the user. The time taken to analyse the dataset can also be extracted from this application.

Chart

Description automatically generated with medium confidence

Screenshot showing application used to apply outlier detection.

The outlier detection methods in the ensemble are implemented using python. These methods work individually first to make a prediction with a confidence score. A voting system, also implemented using python, determines the final classification.

## Hypothesis

The implemented outlier detection method (ensemble) is an effective outlier detector for labelled datasets and will generate good scores for accuracy, precision, recall and f1.

## Methods

The combined predictions of an ensemble of weak classifiers are used as the method to detect outliers in this experiment. These detectors generate a prediction for a piece of data (outlier or inlier), the combined predictions are combined to produce a final classification.

A quick observation shows that the time-of-day affects the data. I.e., CPU usage is higher during typical office hours compared with night-time. To account for this, these datasets are split to hours before the detection is performed. This means there will be no false positive predictions made when the time series moves from daytime to evening, but the idea of concept drift is still considered day to day (due to factors such as new applications being deployed to these EC2 instances) [6].

There are 4 classification techniques in the Ensemble.

* **Moving Average**

This technique uses the average of the previous data points in the time series to classify the next. After the average is calculated, the standard deviation of the previous datapoints is calculated. The standard deviation is used as a threshold, if they next datapoint is less than or greater than the average calculated +/- the threshold then the datapoint is classified as an outlier [7]. The graph shows this technique in practice, the red lines represent the boundaries, and the red dots are the outliers detected.

Chart, line chart

Description automatically generated

Fig. 1 Moving Average outlier detection showing boundaries

* **Moving Median**

This technique follows the same steps as the previous except a median is calculated instead of the average [8]. The graph below shows this technique in practice, observe how the boundaries are like moving average but different outliers have been detected.

Chart, line chart

Description automatically generated with medium confidence

Fig. 2 Moving Median outlier detection showing boundaries

* **Moving Boxplot**

This technique takes several of the previous data points and generates a boxplot. The interquartile range is combined with the upper and lower quartiles to produce a threshold (1.5 \* the inter-quartile range). If the next datapoint is outside the threshold, then the datapoint is classified as an outlier [9].

1st Quartile

3rd Quartile

1.5 \* IQR (Upper bound)

1.5 \* IQR (Lower bound)

Fig. 3 Boxplot Outlier Detection Example

* **Histogram**

This technique plots histograms of subsets of the data. If a range in the histogram has a height less than a defined threshold, then the range is said to contain outliers [10]. If a range has a height below the threshold, but the ranges beside it have a height higher than the threshold then it is considered a borderline inlier.

**Chart

Description automatically generated**

Fig. 4 Histogram Based Outlier Detection

**Voting on a Final Classification**

These techniques run individually first, generating a prediction and a ‘confidence’ score. The confidence scores are combined to generate a final prediction. The formula behind this voting mechanism is described below.

Confidence is calculated by the distance between a datapoint and the threshold.

For predictions, -1(outlier) and 1(inlier), the above equation computes a minimum prediction of -n and a maximum of n. By visualising possible outputs on a spectrum, it can be said that an outlier score < 0 is likely to be an actual outlier.

0

N (max inlier)

-N (min outlier)

**Method of Scoring the Detector**

The datasets being analyzed have been labelled by the Numenta Anomaly Benchmark (NAB). NAB is a platform for testing detection techniques on timeseries data. It contains 58 labelled datasets used for scoring algorithms [11]. Labelling data is expensive [12], but these datasets are available for free from NAB and are crucial to this experiment.

The software used to perform the experiments uses the labels provided by NAB to plot the outlier areas. The graph below shows some timeseries data with areas containing outliers marked by red rectangles.

Graphical user interface, application, Teams

Description automatically generated

Fig. 5 Graph demonstrating how the application represents outlier areas.

The software calculates four metrics to determine the overall performance of the detector, accuracy, precision, recall and f1 score. These are calculated using the following equations.

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |

Equations used to evaluate the detector against the dataset

## Results

The ensemble of outlier detector methods run on the CPU data. For these results, the voting with ‘confidence’ score is used.

|  |  |
| --- | --- |
| Chart, histogram  Description automatically generated | Chart  Description automatically generated |
| I. Detection result for Numenta VM1 | II. Detection result for Numenta VM2 |
| A graph with red and blue lines  Description automatically generated with low confidence | Chart, bar chart  Description automatically generated |
| III. Detection result for Numenta VM3 | IV. Detection result for Numenta VM4 |
| Chart  Description automatically generated | Chart  Description automatically generated |
| V. Detection result for Numenta VM5 | VI. Detection result for Numenta VM6 |
| Chart  Description automatically generated | Chart  Description automatically generated with medium confidence |
| VII. Detection result for Numenta VM7 | VIII. Detection result for Numenta VM8 |

Chart

Description automatically generated

IX. Detection result for Numenta VM9

Fig. 6 Graphs showing CPU utilization over time with outlier detection

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| VM NAME | Accuracy | Recall | Precision | f1 | Run time |
| Numenta VM1 | 90.1 | 100.0 | 80.0 | 88.9 | 6.4936 |
| Numenta VM2 | 51.3 | 100.0 | 18.5 | 31.3 | 6.7717 |
| Numenta VM3 | 31.3 | 100.0 | 17.6 | 30.0 | 6.967 |
| Numenta VM4 | 87.6 | 100.0 | 24.6 | 39.5 | 6.5469 |
| Numenta VM5 | 91.9 | 100.0 | 58.5 | 73.8 | 7.6593 |
| Numenta VM6 | 91.7 | 100.0 | 83.0 | 90.7 | 7.1889 |
| Numenta VM7 | 53.2 | 0.0 | 0.0 | 0.0 | 7.262 |
| Numenta VM8 | 90.0 | 50.0 | 49.2 | 49.6 | 7.6805 |
| Numenta VM9 | 90.3 | 100.0 | 73.7 | 84.8 | 8.1605 |
| Average | 75.3 | 93.8 | 50.6 | 61.1 | 7.1923 |

* Numenta V 7 excluded from averages because no true positives thereof no f1 score

Performance of individual detectors

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Average | Median | Boxplot | Histogram |
| Numenta VM1 | 66.7 | 57.1 | 42.1 | 37.1 |
| Numenta VM2 | 30.4 | 30.8 | 43.3 | 60.6 |
| Numenta VM3 | 30.9 | 30.6 | 26.2 | 45.7 |
| Numenta VM4 | 32.1 | 46.5 | 45.6 | 30.7 |
| Numenta VM5 | 50.4 | 52.7 | 62.6 | 99.7 |
| Numenta VM6 | 66.7 | 91.8 | 88.3 | 59.3 |
| Numenta VM7 | 0 | 0 | 0 | 0 |
| Numenta VM8 | 66.7 | 44.9 | 58.7 | 66.7 |
| Numenta VM9 | 66.7 | 61.5 | 56.4 | 82.2 |
| Average | 51.325 | 51.9875 | 52.9 | 60.25 |

Naming convention to put in appendix

|  |  |  |
| --- | --- | --- |
| S/No | VM ID | VM NAME |
| 1 | ec2\_cpu\_utilization\_5f5533 | Numenta VM1 |
| 2 | ec2\_cpu\_utilization\_24ae8d | Numenta VM2 |
| 3 | ec2\_cpu\_utilization\_53ea38 | Numenta VM3 |
| 4 | ec2\_cpu\_utilization\_77c1ca | Numenta VM4 |
| 5 | ec2\_cpu\_utilization\_825cc2 | Numenta VM5 |
| 6 | ec2\_cpu\_utilization\_ac20cd | Numenta VM6 |
| 7 | ec2\_cpu\_utilization\_c6585a | Numenta VM7 |
| 8 | rds\_cpu\_utilization\_cc0c53 | Numenta VM8 |
| 9 | rds\_cpu\_utilization\_e47b3b | Numenta VM9 |

## References

[1] AWS Amazon. (2022). *Amazon EC2 – Secure and resizable compute capacity for virtually any workload* [Online]. Available: <https://aws.amazon.com/ec2/>

[2] AWS Amazon (2022). *Monitor Amazon EC2* [Online]. Available: <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/monitoring_ec2.html>

[3] Ionos (2020, Feb. 24) *High CPU usage: What does this mean?* [Online]. Available: <https://www.ionos.com/digitalguide/server/know-how/cpu-usage/>

[4] Sasaki, Yutaka. (2007). The truth of the F-measure. Teach Tutor Mater. Available: <https://www.researchgate.net/publication/268185911_The_truth_of_the_F-measure>

[5] T. Wood. (n.d.) Machine Learning Glossary and Terms – F-Score [Online]. Available: <https://deepai.org/machine-learning-glossary-and-terms/f-score>

[6] Tsymbal, Alexey. (2004). *The problem of concept drift: definitions and related work*. Computer Science Department, Trinity College Dublin 106.2: 58. <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.58.9085&rep=rep1&type=pdf>

[7] Dr. Dataman. (2021, Apr, 18). *Anomaly Detection for Time Series. (1) Simple Moving Average.* [Online]. Available: [https://medium.com/dataman-in-ai/anomaly-detection-for-time-series-a87f8bc8d22e](file:///C:\Users\lreid\outlier-detection-in-virtual-machines\resources\%20https:\medium.com\dataman-in-ai\anomaly-detection-for-time-series-a87f8bc8d22e)

[8] Anomaly. (2016, Jan. 12). *Detecting Anomalies with Moving Median Decompsition*. [Online]. Available: <https://anomaly.io/anomaly-detection-moving-median-decomposition/index.html>

[9] Andrea, Kliton & Shevlyakov, Georgy & Smirnov, Pavel. (2013). *Detection of outliers with boxplots*. 141-144. <https://www.researchgate.net/publication/261173084_Detection_of_outliers_with_boxplots>

[10] Goldstein, Markus & Dengel, Andreas. (2012). *Histogram-based Outlier Score (HBOS): A fast Unsupervised Anomaly Detection Algorithm*. Available: <https://www.goldiges.de/publications/HBOS-KI-2012.pdf>

[11] Numenta. (2015). *The Numenta Anomaly Benchmark – White Paper.* 1. Available: [https://numenta.com/assets/pdf/numenta-anomaly-benchmark/NAB-Business-Paper.pdf#:~:text=The%20Numenta%20Anomaly%20Benchmark%20%28NAB%29%20is%20an%20open,NAB%3A%20the%20labeled%20dataset%20and%20the%20scoring%20system.](https://numenta.com/assets/pdf/numenta-anomaly-benchmark/NAB-Business-Paper.pdf%23:~:text=The%20Numenta%20Anomaly%20Benchmark%20%28NAB%29%20is%20an%20open,NAB%3A%20the%20labeled%20dataset%20and%20the%20scoring%20system.)

[12] Cloudfactory. (n.d.). *The Ultimate Guide to Data Labelling for Machine Learning* [Online] Available: <https://www.cloudfactory.com/data-labeling-guide>