Machine Learning for Anomaly Detection

PATEL VEDANT

March 2024

1 Introduction

Machine learning anomaly detection is like having this neighbor on steroids! The key is to train computers to identify common patterns and behaviors in your data, such as the rhythm of network traffic, the beat of a machine, or the flow of financial transactions. But here's where the fun starts: these smart algorithms raise their virtual eyebrows and exclaim, "**Aha!** "when something unusual occurs, such as an abrupt rise in transactions or a strange blip in sensor readings.

The process of spotting unusual occurrences or observations that can cause suspicion because they differ statistically from the majority of observations is known as anomaly detection. Such "anomalous" behavior usually indicates the presence of an issue, such as a cyberattack or a failed server, etc.

2 Methods and Types

An anomaly can be mainly categorized into the following categories –

1. Point Anomaly: A dataset's point anomalies are tuples that deviate significantly from the rest of the dataset.
2. Contextual Anomaly: An observation qualifies as a contextual anomaly if its context makes it unusual.
3. Collective Anomaly: An anomaly can be found by combining a number of data examples.

Machine learning methods can be applied to anomaly detection in the following ways.

Supervised Anomaly Detection: For this method to build a prediction model that will categorize future data points, a labeled dataset comprising both normal and anomalous samples is required. Supervised neural networks, support vector machine learning, the K-Nearest Neighbors Classifier, and other methods are most frequently employed for this purpose.

Unsupervised Anomaly Detection: This technique does not require any training data; instead, it assumes that Very little of the data is abnormal and Every

anomaly deviates statistically from the normal samples. The data is then clustered using a similarity metric based on the previously mentioned hypotheses, and the data points that are far from the cluster are regarded as anomalies.

3 Data Preprocessing

Cleaning and preparing the data to make it appropriate for examination by the anomaly detection algorithms is known as data preprocessing, and it is an essential step in the anomaly detection pipeline.

Data Cleaning:

Managing Missing Values: Recognize and address the dataset's missing values. This could involve eliminating rows or columns that contain missing data when appropriate, or it may include assigning missing values using methods like mean, median, or mode imputation.

Deleting Duplicate Entries: If there are duplicate rows in the dataset, look for them and delete them.

Scaling and Normalization of Features:

Standardization: Assign a mean of 0 and a standard deviation of 1 to the features. This prevents the study from being dominated by features with bigger scales. *Normalization:* involves adjusting characteristics to a range of 0 to 1. This is very helpful for distance-measuring algorithms like SVM and k-NN.

Selecting and Extracting Features:

Feature Selection: Select pertinent features that will help with the anomaly detection task. This might involve choosing features based on subject expertise or evaluating feature importance scores.

Feature extraction: involves transforming or creating new features from the ones that already exist to extract more valuable data. For dimensionality reduction and feature extraction, methods such as principal component analysis (PCA) or t-distributed stochastic neighbor embedding (t-SNE) can be employed.

Data Conversion:

Managing Categorical Variables: Use methods such as label encoding or one-hot encoding to encode categorical variables into numerical representation.

Managing Skewed Data: If skewness exists in the feature distribution, use methods like log transformation or Box-Cox transformation to address it.

Data discretization involves either binning or discretizing the values of continuous features to turn them into categorical ones.

Handling Unusual Data:

Finding Outliers: Use statistical techniques or domain-specific expertise to find and manage outliers in the data.

Outlier Treatment: Depending on how an outlier affects the analysis, decide whether to eliminate it, replace it with a more typical value, or leave it in place.

Data Splitting:

Train-Validation-Test Split: To reliably assess the anomaly detection model's performance, divide the dataset into distinct sets for training, validation, and testing.

4 Anomaly Detection Techniques

4.1 Unsupervised Anomaly Detection Techniques

- Statistically based Methods: To identify outliers, use statistical features like mean and standard deviation. Dixon's Q Test, Grubbs' Test, and Z-Score are a few examples.
- Distance-based Methods: To identify anomalies, calculate the distances between data points. Local Outlier Factor (LOF) and k-Nearest Neighbors (k-NN) are two methods.
- Based on density Methods: Use variations in data density to identify anomalies. DBSCAN and Gaussian Mixture Models (GMM) are two examples.

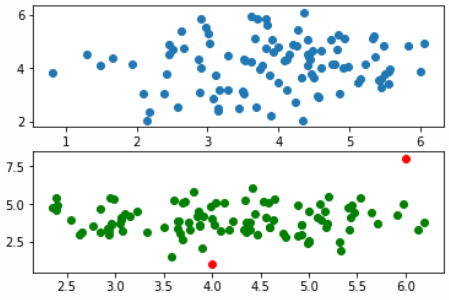

Figure 1: Unsupervised Learning

4.2 Supervised Anomaly Detection Techniques

- Support vector machines (SVM): Determine the boundary that separates typical data from unusual data.
- Isolation Forest: In a decision tree forest, isolate anomalies by causing fewer splits.
- One-Class SVM: Recognize the bounds of normal data and identify cases that fall outside of them.
- Neural Networks (Autoencoders): Utilize training data that is typical in order to reconstruct it and detect abnormalities based on increased reconstruction mistakes.

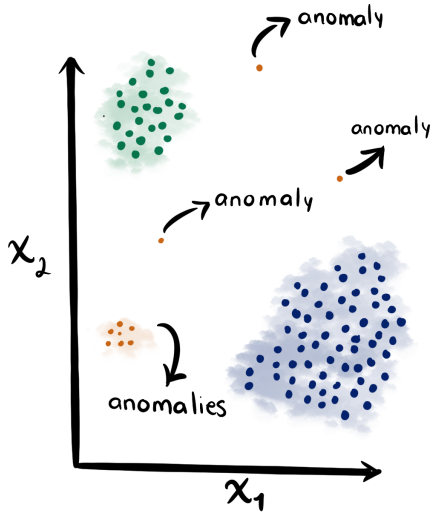

Figure 2: Supervised Learning

4.3 Semi-Supervised Anomaly Detection Techniques

- Self-training: Combine high-confidence predictions into iterative training on both labeled and unlabeled data.
- Co-training: Exchange highly confident predictions while training multiple models on various data perspectives.

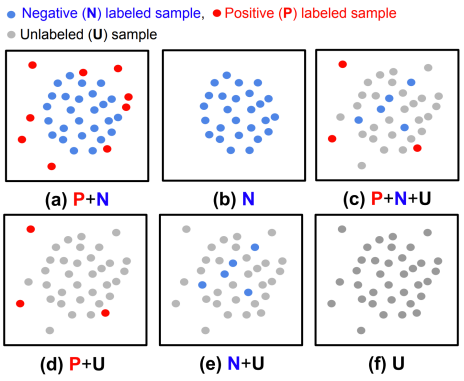

Figure 3: Anomaly results using all techniques

5 Evaluation Metrics for Anomaly Detection

They are essential for evaluating anomaly detection algorithms' performance. They aid in measuring the degree to which a model can discern between typical and unusual occurrences within the dataset.

Evaluation metrics:

- True Positive (TP): Correctly identified anomalies.
- False Positive (FP): Normal instances incorrectly classified as anomalies.
- True Negative (TN): Correctly identified normal instances.
- False Negative (FN): Anomalies incorrectly classified as normal.

		Actual Class	
		Positive (**P**)	Negative (**N**)
Predicted Class	Positive (**P**)	True Positive (**TP**)	False Positive (**FP**)
	Negative (**N**)	False Negative (**FN**)	True Negative (**TN**)

Figure 4: Confusion Matrix

Derived metrics:

- Accuracy: Overall correctness of the model.
- Precision: Proportion of correctly identified anomalies among all classified.
- Recall (Sensitivity): Ability to identify all actual anomalies.
- F1-score: Harmonic mean of precision and recall.
- Receiver Operating Characteristic (ROC) curve: Trade-off between true positive rate and false positive rate. The model performs better the closer the curve is to the upper-left corner. A curve that approaches the diagonal line indicates that the model performs no better than random guesswork.
- Area Under the Curve (AUC): Overall performance of the model. Better performance is indicated by a larger AUC value; a classifier with an AUC of 1 is ideal, whereas one with a value of 0.5 is no better than random guessing.

Precision (P)	$\frac{\text{TP}}{\text{TP+FP}}$
Recall (R)	$\frac{\text{TP}}{\text{TP+FN}}$
F1-score	$2 \times \frac{P \times R}{P+R}$
Accuracy	$\frac{\text{TP+TN}}{\text{TP+TN+FP+FN}}$

Figure 5: Formulas

6 Examples and Cases

Identifying Credit Card Fraud: When a lot of valid transactions occur, financial institutions use anomaly detection to find fraudulent ones. Transaction data is analyzed by anomaly detection algorithms, which search for odd trends like significant transactions in odd places or erratic spending patterns.

Example: Usually, a credit card user uses it to make minor local purchases. The system may flag a significant transaction from a foreign nation as abnormal and subject to further investigation if it occurs suddenly.

Monitoring of Healthcare: In the medical field, anomaly detection is utilized to track patient information and identify deviations that can point to a decline in health or possible medical crises. Vital signs, test results, and other health variables are analyzed by algorithms for anomaly identification, which searches for departures from typical patterns or ranges.

Example: In a hospital, the monitoring system may notify medical professionals to look into a patient's condition more thoroughly if their heart rate abruptly increases or decreases considerably from normal ranges.

Detection of Network Intrusion: Anomaly detection in cybersecurity aids in identifying unusual network activity suggestive of a possible intrusion or attack. When analyzing network traffic, anomaly detection algorithms search for odd patterns like an abrupt increase in data movement or unauthorized access attempts.

Example: the system might flag an attempt to access the network late at night by a system administrator who typically uses it during regular office hours as suspicious.

Identifying False Insurance Claims: Insurance firms use anomaly detection to separate out claims that might be fraudulent from those that are genuine. Algorithms examine a number of claim parameters, including the amount of the claim, the applicant's past, and the specifics of the occurrence, in an effort to find anomalies or inconsistent patterns.

Example: The system may identify these as possible fraudulent behaviors if a person makes several claims for the same incidents in a short amount of time or gives inconsistent information in each claim.

7 WorkFlow of anomaly detection:

The detailed method of utilizing machine learning algorithms for anomaly detection is illustrated in the workflow that follows. The process of creating, enhancing, testing, and implementing an anomaly detection model is shown in this chart. Every step of the workflow includes important tasks, such as selecting, training, and evaluating models in addition to data gathering and preprocessing. Organizations may create strong anomaly detection systems that can efficiently find and address anomalies in a variety of domains by adhering to this organized process. The flowchart facilitates a clear understanding of the underlying workflow by acting as a visual guide and describing the important phases and decision points involved in the anomaly detection process.

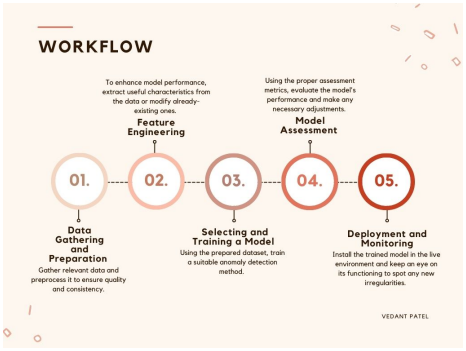

Figure 6: Workflow of ML in Anomaly Detection

8 Conclusion

In conclusion, machine learning-based anomaly identification offers a potent method for locating oddities or outliers in datasets from a variety of fields. Organizations can detect abnormalities in batch or real-time processing settings by utilizing advanced algorithms and approaches. This allows for prompt action and mitigation of any risks or threats. Building, training, assessing, and implementing anomaly detection models may be done in an organized manner with the help of the described systematic workflow, which guarantees robustness and efficacy in identifying abnormalities while reducing false positives and false negatives. Research and innovation in anomaly detection will propel the creation of more precise, scalable, and adaptable solutions, improving the capacity to protect systems, assets, and operations from unanticipated deviations, as issues change and technology advances.