# Unsupervised Anomaly Detection

## – Model and feature manipulation to predict specific anomalies

Aravindh Sankar Ravisankar

School of Mathematics, University of Edinburgh, Edinburgh, U.K. **Poster Code: C11** s2596860.ed.ac.uk

## 1. Introduction

The research work aims to develop an **unsupervised anomaly detection model** for **effectively capturing risk events** which could potentially replace traditional human detection methods. The model seeks to go beyond basic anomaly detection, providing companies with a more precise and actionable strategy for managing potential risks.

## 2. Data

The dataset comprises longitudinal and multivariate spending data with **105,277 records** spanning from **January 2023 to April 2023**. It encompasses **10 feature columns** across **2185 unique individuals**. Data preprocessing is performed to exclude records that had no associated amount. The data is primarily made up of continuous features with "department" being the sole categorical feature. The **target variable** is **"at_risk_event"** which takes binary values of True or False. Other significant variables of interest include "spend", "individual_id", and "date". The dataset's structure requires the application of robust feature engineering techniques to derive temporal features. As a result, various aggregate and rolling window features were created.

## 3. Exploratory Data Analysis

The analysis of some feature variables revealed the following key insights:

- At first, risk ratio analysis is conducted on the day-wise aggregated data.
- Over the weekdays, we can observe that the aggregated spending is higher whereas the corresponding risk ratios are lower.
- On the contrary, aggregated spending significantly drops over the weekend while the risk ratio increases sharply.
- The overall pattern clearly shows a **negative correlation** between **aggregated spending** and the **risk ratio** highlighting the need for **careful risk monitoring** during the **weekend**.
- Secondly, the data is aggregated by the hour of the transaction followed by a risk ratio analysis.
- The risk ratio peaks around midnight **(12:00 AM)** followed by a significant decline, reaching a new low around 7:00 AM.
- It remains stable over an extended period followed by a steady increase again after 6:00 PM.
- This pattern indicates **higher risk outside typical business hours** which emphasizes the need for enhanced monitoring and risk management strategies during out-of-office hours.

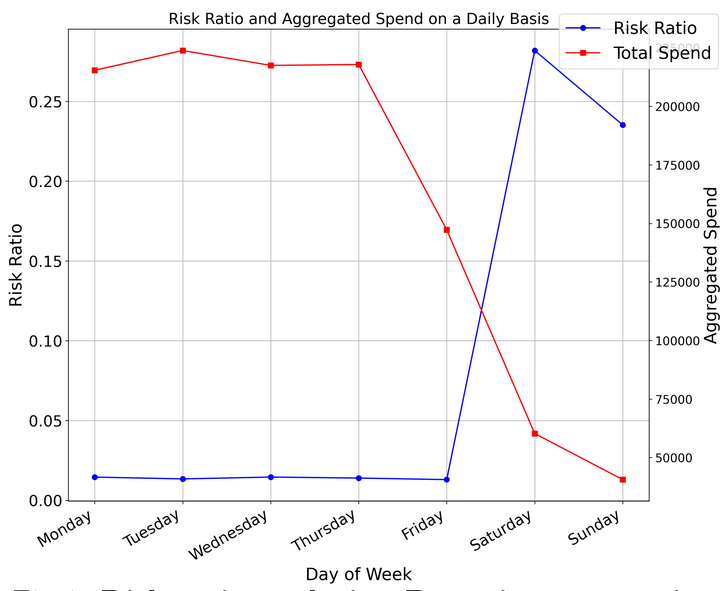


Fig 1. **Risk ratio analysis - Day wise aggregation**

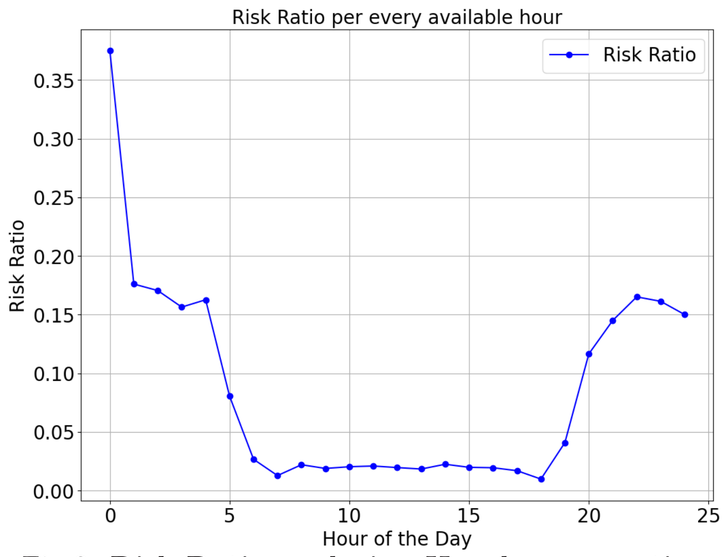


Fig 2. **Risk Ratio analysis - Hourly aggregation**

## 4. Modeling

- **Isolation Forest** operates on the assumption that anomalies are rare and distinct. It builds binary trees using random feature splits to isolate data points. Anomalies have shorter path lengths requiring fewer splits while normal data points have longer paths. The anomaly score is calculated using the below formula:

$$s(x, n) = 2^{-\frac{E(h(x))}{c(n)}}$$

- **One-class SVM** operates by learning a decision function for the normal data and identifying data points outside this boundary as anomalies. It achieves this by mapping the input data into a higher dimensional feature space and finding the optimal hyperplane that effectively distinguishes normal data points from potential anomalies. The primary objective is given as:

$$\min_{w,\xi,\rho} \quad \frac{1}{2}\|w\|^2 - \rho + \frac{1}{\nu n}\sum_{i=1}^{n}\xi_i$$

- Long Short-Term Memory networks handle long-term dependencies with their gated architecture.**LSTM Autoencoders** leverage this model for anomaly detection by compressing the input data into a lower-dimensional latent space and then reconstructing it back to the original dimension. The model captures essential features of the data by minimizing the reconstruction error which is given as follows:

$$L = \frac{1}{2}\sum_{x}\|x - \hat{x}\|^2$$

## 5. Results and Inferences

Our results and inferences suggest:

- **Isolation Forest** has a **high recall** indicating that the model is effective at identifying most of the actual risk events but a low precision value highlighting a significant number of false positives.
- The **One-Class SVM** model achieves a slightly higher F1-score and a better **balance** between **precision and recall** than the Isolation Forest indicating moderate effectiveness in distinguishing between normal and risk events.
- **LSTM AutoEncoder** excels with the **highest AUC and AUPR scores** demonstrating strong discriminatory power between normal and risk events despite its lower precision and recall measures.
- Overall, the **LSTM Autoencoder** is **highly recommended** for its better balance across metrics, effectively distinguishing true risk events with fewer false positives.

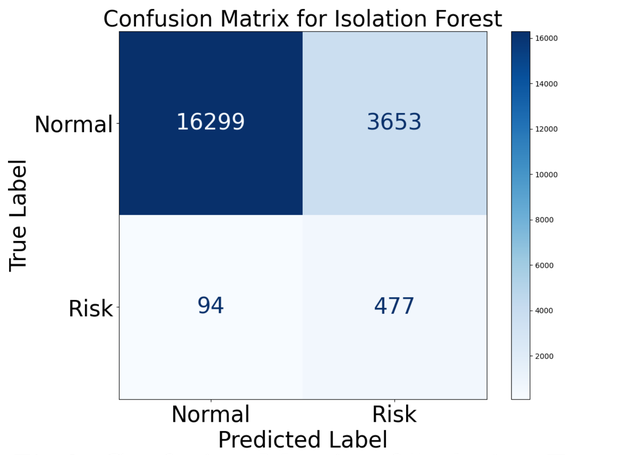


Fig 3. **Confusion Matrix of Isolation Forest**

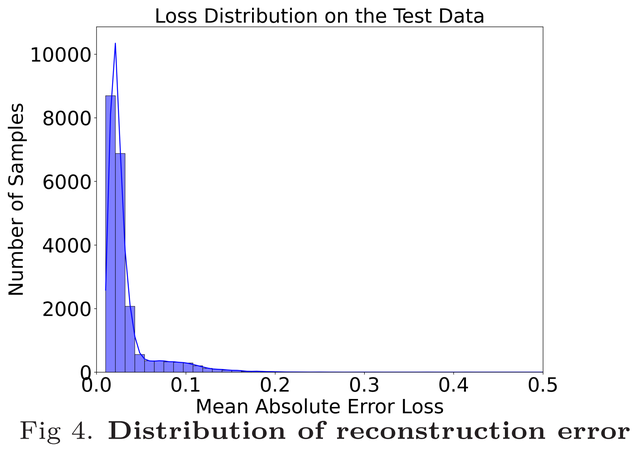


Fig 4. **Distribution of reconstruction error**

## 6. Further Research

- Explore the potential of hypernetworks in handling varied transaction counts across individuals.
- Deploying composite models for enhanced accuracy and reliability.

## 7. References

[1] Mohiuddin Ahmed, Abdun Naser Mahmood, and Jiankun Hu. A survey of network anomaly detection techniques. *Journal of Network and Computer Applications*, 60:19–31, 2016.

[2] Waleed Hilal, S Andrew Gadsden, and John Yawney. Financial fraud: a review of anomaly detection techniques and recent advances. *Expert systems With applications*, 193:116429, 2022.