Analyzing Anomalies for Financial Fraud Detection: A Case Study of Selected Insurance Companies Listed in Borsa Istanbul

Muhammad Nouman Latif[1]
Muhittin Kaplan[2]
Asad Ul Islam Khan[3]

Abstract:

This study aims to detect financial fraud by identifying anomaly in the financial data (i.e, listed insurance companies in Borsa Istanbul, Turkiye). Traditional anomaly detection methods like GARCH, ARIMA and moving averages have shortcoming i.e., data should be stationary, must follows a specific distribution and avoid mis-specification of model. In order to coupe with these problems, we use four different measures of risk i.e., Down-to-Up Volatility (DUV), Negative Conditional Skewness (NCS), Relative Frequency (RF) and the Garman-Klass (GK) on Daily data of six leading insurance companies listed in Borsa Istanbul to uncover anomalies. These four measures of risk are directly computed from the data so the problem of stationarity and misspecification of distribution/model will not occur. The results highlighted the key differences among the methods, as DUV and RF are based on the second moment, GK approach for risk is calculated on daily basis and NSK is based on the third moment, so they detect different number of anomalies as well. To ensure more comprehensive analysis, we employ Z score and Mahalanobis distance to capture anomalies in our dataset, enhancing the robustness of our finding. As the Z Score Normalization treats each risk measure, equally that enables it suitable for normally distributed data. However, it does not account for potential correlations among the risk measures and may overlook overlapping effects. Whereas, Mahalanobis distance perform better due to its nature of considering non-normally distributed data, multivariate anomalies and correlation between the risk measures. Given its ability to incorporate correlations between risk measures and detect joint anomalies, the Mahalanobis distance-based approach provides a more holistic and reliable identification of anomalies in our analysis. The study concluded that there are different anomalies in the six listed insurance companies at Borsa-Istanbul, while using these four measures of risk. Hence, based on Mahalanobis distance and Z score normalization, it was concluded that Mahalanobis distance has detected better number of anomalies as compare to Z Score normalization for five listed insurance companies except RAYSG.

Key words: Anomaly detection, financial fraud, market spillover, Stock Market

1. Introduction:

Financial fraud has remained a persistent challenge for global economies, affecting not only financial markets but also eroding investor confidence and harming corporate integrity. Therefore, it is necessary to promote and develop resilient financial system that facilitate the allocation of capital, risk management and financial intermediation. This objective is supported by a diverse range of financial institutions and markets that enable these fundamental activities and ensure the efficient flow of funds among investors, borrowers and saver. These financial system include Market-based, bank-based, digital and decentralized frameworks. Each playing a crucial role in maintaining financial stability and promoting economic growth. From above-mentioned four financial systems the Market-based is the most dominant (Svitlana, Y., & Kostiantyn, H. (2023). In the market based system, there are Stock markets, bonds market and Foreign exchange rate market. However, the role of stock markets is very crucial due to their inherently extreme volatile nature. This extreme volatility often results in data that is not only highly fluctuating but also skewed and influenced by behavioral biases. Understanding these characteristics is essential for making informed investment decision, ensuring market stability and enhancing fraud detection mechanisms.

Before fraud detection, we have to know its kinds in stock market i.e., pump and dump, false market conditions, accounting fraud and insider trading. Firstly, the infamous "pump and dump" schemes typify market manipulation, where a group of traders hypes up a stock to inflate its price before selling it off, leaving other investors to face subsequent price drops (Lee, E. J., et al. 2023; La Morgia, M., et al. 2023). Second type manipulation that includes creating “false market conditions” through

[1] PhD Candidate, Department of Economics, School of Business, Ibn Haldun University, Istanbul, Turkiye (muhammad.latif@stu.ihu.edu.tr) https://orcid.org/0000-0002-3055-7729

[2] Professor, Department of Economics, School of Business, Ibn Haldun University, Istanbul, Turkiye (muhittin.kaplan@ihu.edu.tr) https://orcid.org/0000-0002-0685-7641

[3] Assistant Professor, Department of Economics, School of Business, Ibn Haldun University, Istanbul, Turkiye (asad.khan@ihu.edu.tr) https://orcid.org/0000-0002-5131-577X

wash trading or spoofing, where traders place orders they have intention to deceive others about stock demand (Comerton-Forde & Putniņš, 2014). Thirdly, Insider trading, those with privileged information about a company's future performance or strategic plans perpetrate this form of fraud. They exploit this information for personal gain by trading the company's stock before the information becomes public. Although insider trading laws exist, sophisticated detection mechanisms are essential to identify and deter such actions effectively (Seyhun, 1986; Abdulrhman, Alqurayn., et al., 2024). Lastly, Accounting fraud, when someone changes a company's financial records, usually by lying about earnings or asset growth.

These fraudulent practices have serious consequences, often these results in significant stock mispricing, leading to harm uninformed investors. For instance, Enron and WorldCom are two examples of cases that prove the risk of unregulated accounting manipulations and the necessity of strict fraud detection procedures (Dechow, Ge, & Schrand, 2010). Therefore, detecting financial fraud is most important thing to maintain the integrity of financial markets. As the fraudulent activities weaken the investor confidence; can mislead the market dynamics, which can result in financial loss for both investor and the companies. If these fraudulent activities remains undetected, they can not only harm stakeholders but also destabilize the financial system (Wells, 2017). Financial anomalies consist of unexpected volatility surges, which can occur due to human error, fraudulent activities, behavioral changes or fault within the system (Hodge & Austin, 2004). Consequently, it is important to develop mechanisms for identifying financial fraud to ensure transparency and fairness in the market. Potential financial fraudulent activities can be observed through anomalies or unusual patterns in financial data (Chandola et al., 2009; Hawkins, 1980). One of the widely used approach to detect financial fraud is through anomaly detection methods. These methods aims to identify irregular patterns in financial data, which can result in fraudulent activity. Anomaly detection been used in many domains including finance to find suspicious transactions, manipulative trading or misreported financial information (Lee, E. J., et al. 2023; La Morgia, M., et al. 2023; Fahlevie, R. A., et al. 2022).

The use of traditional statistical/model based anomaly detection methods is very limited in the literature due to their limitations. A key limitation lies in their assumption about nature of data, such as normality or stationarity, which are often violated in financial datasets (Li, Y., & Zhang, X., 2023). These models like ARIMA, ARCH and GARCH, are designed to capture volatility patterns usually struggle when applied to high frequency data . Moreover, general weakness of these methods includes their inability to detect false positive and struggle to handle large dataset efficiently (Smith & Johnson, 2020). To deal with these challenges, our study proposes leveraging Measures of risk as an innovative approach to detect anomalies and, by extension, potential fraud within the context of insurance companies listed in Borsa-Istanbul. These measures of risk offer many advantages over traditional methods, as they are distribution free, no model assumption (Linear / non-linear) and they are finding volatility directly from data, so there is no problem of induced volatility.

Our study uses four different volatility measures to detect anomalies, who are different in approach and in their philosophy. Firstly, Down-to-Up (variation in the positive and negative returns in a month) is a measure of volatility, which represents the disparity between upward and downward price movements and in the past has been useful in capturing, abnormal price action that could be construed as fraudulent activities (Brockman et al., 2017). Second approach also widely used is the GK measure of risk (captures the intra-day volatility), used to estimate the total risk exposure in the portfolio or market or within a particular sector by specifying the extreme market conditions and potential outliers, which leads to identification of deviations relating to fraudulent activities (Haykir, O., & Yagli, I., 2022). These two techniques based on risk/volatility; therefore, these are the approximations of second moment of the distribution. Besides, third moment analyses the excess kurtosis in the assets returns prices. It offers a better identification of market anomalies because it considers the marginal nature of the return distribution (Zhang et al., 2020). Therefore, Third useful indicator for anomaly detection is Negative Conditional Return Skewness (NCRS) – the skewness of returns conditioned on negative returns. This measure aims at the very low end which sometimes results from mergers or other questionable activities in the year of crises (Xu, Z., Li, X., Chevapatrakul, T., & Gao, N. (2022). Another measure (4^{th}) that can be used for anomaly detection is the RF, which is the relative frequency of crash days in a month. The 3^{rd} and 4^{th} measures are used as crash risk measures in the literature (Piotroski, J. D., Wong, T. J., & Zhang, T. (2015) and they are approximations of the 3^{rd} moment of the distribution. After estimating our four risk measure we are looking to have more comprehensive results, so we combine the effect of all these four risk measures by using i) Z score normalization (Jain, A., et al., 2005) and ii) Mahalanobis distance (Flores-Guerrero, J. L., et al., 2021) to find joint anomaly detection, then the results will be more appropriate and reliable.

2. Review of literature

Financial fraud is a criminal act that involves the provision of misleading information on the company's balance sheets or other financial statements or carrying out of unauthorized financial transaction for achieving a certain goal. Such activities may include what could be regarded as manipulation of records in enterprises such as accounting fraud, embezzlement and other forms of financial deception (Senvar, O., & Hamal, S. (2022). The need for identification of financial fraud is therefore paramount to uphold the market integrity and prevent the financiers and competitors from been defrauded. If fraud remains undetected, then organizations suffer increased financial losses, expose themselves to legal liabilities and cause the public to lose confidence in the financial markets (Wells, 2017). Besides, it also reduces the specific risks and prevents the recurrence of fraud, and further maintain the compliance of financial regulations (Ameyaw, M. N., Idemudia, C., & Iyelolu, T. V. (2024). Consequently, statistics and machine learning are now considered crucial in spotting fraudulent behavioural patterns and containing their impact (Kamini, Pareek., et al., 2023).

Fraud detection in the financial systems altogether has an element of dependency on anomalies because fraud works within a system in a way that it deviates from the usual patterns of data, transactions, or other behaviors. Such discrepancies as trade volume, price, and financial statement disparity are suggestive of manipulative fraud such as market manipulation and insider trading, or financial statement fraud (Brockman et al., 2017; Brennan, N. M., & McGrath, M. (2007). Identifying these anomalies, is essential not only in avoiding such risks but also in ensuring that markets maintain their specific standards (Zhang et al., 2020). For instance, insider trading causes price changes which differ with historical trends and which should thus be flagged as outliers (Rozeff, M. S., & Zaman, M. A. (1998). Likewise, fraudulent reporting of financial statements may affect some essential value, including earnings or revenue so that these discrepancies may be identified through the anomaly detection (Lokanan, M., Tran, V., & Vuong, N. H. (2019).

These also make the argument that irregularities may indicate more complex fraud schemes that take advantage of weaknesses in financial markets or systems to obtain their desired outcomes, with the exception of manipulating financial data; for instance pump-and-dump schemes or even Ponzi schemes (Rozeff, M. S., & Zaman, M. A. (1998). Anomaly detection means a possibility of identifying hidden fraud patterns depending on statistical and machine learning patterns; it helps prevent fraud before they progress (Groll, A., Khanna, A., & Zeldin, L. (2024). It is possible to mitigate fraud through a proactive approach, which will benefit financial institutions and regulators by providing real-time detection and preventive measures', increasing the efficiency and stability of the markets (Brockman et al., 2017; Zhang et al., 2020). In other words, anomaly detection remains an essential component of the contemporary fraudulent detection models as they can identify financial crimes that are likely to go unnoticed in good time (Lokanan, M., Tran, V., & Vuong, N. H. (2019).

Techniques that measure irregular actions within the different attributes of volatility, risk measures as well as the properties inherent with their distribution have become more prevalent because they are effective in the identification of an abnormal condition within the financial market. This means that there is a consensus in the literature that the anomaly detection refers to financial fraud detection. However, the methods of identifying anomalies vary across studies as different methods are used to detect anomalies, some of them are based on AI and machine learning and some of them are traditional statistical methods. In our study, based on consensus in the literature, we are also using anomaly detection as an indicator / signal of financial fraud detection. However, we are using four different methods of risk measures that we can use for anomaly detection and all these four methods are from the family of traditional statistics.

These measures of risk are distinct from general anomaly detection approaches, as they detect anomalies from the data directly and avoid model specification problems and not relying on a few selected financial assets or a linear correlation coefficient. Furthermore, they are capturing the second moment, third moment as well as the daily risk in the stock exchange dataset. So our measures of risk models like Down-to-Up volatility, Relative Frequency or NCRS focus on movements of the market abnormalities or great risks (Chen et al., 2001; Piotroski, J. D., Wong, T. J., & Zhang, T. (2015).

3. Methodology

In this section, we briefly described the data series, estimation techniques of four anomaly detection methods and comparison approaches.

3.1. Data

The study will utilize daily transactional data from Türkiye's stock exchange, encompassing stock opening and closing prices, high and low prices (for GK analysis of price fluctuations), and returns (as measures of relative dispersion for volatility and skewness). Analyzing data from banks, insurance firms, leasing companies, and holding and investment companies is critical due to the distinct nature of financial fraud risks faced by each sector. Considering the distinct nature of volatility of all these companies, current study focuses only on the insurance companies. Insurance companies often contend with fraudulent or exaggerated claims and policy scams, which can involve complex schemes that challenge anomaly detection systems designed to monitor irregular claim patterns (Palacio, 2019).

For the study, daily data from January 2010 to October 2024 of six leading Insurance companies (AGESA Hayat Ve Emeklilik A.Ş., AK Sigorta A.Ş., Anadolu Hayat Emeklilik A.Ş., Anadolu Anonim Türk Sigorta Şirketi, RAY sigorta A.Ş., Türkiye Sigorta A.Ş.) listed in Borsa Istanbul (BIST-100) has been used.

Figure 1

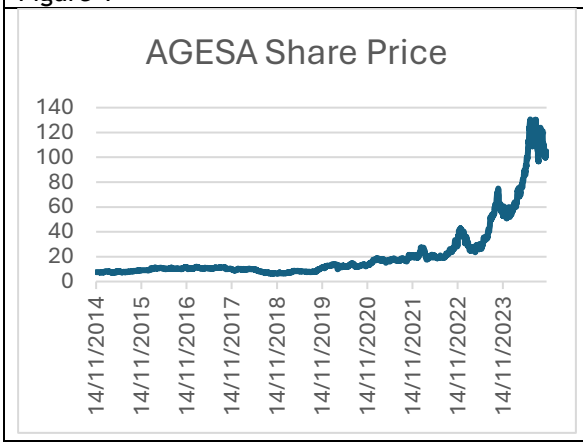


Figure 2

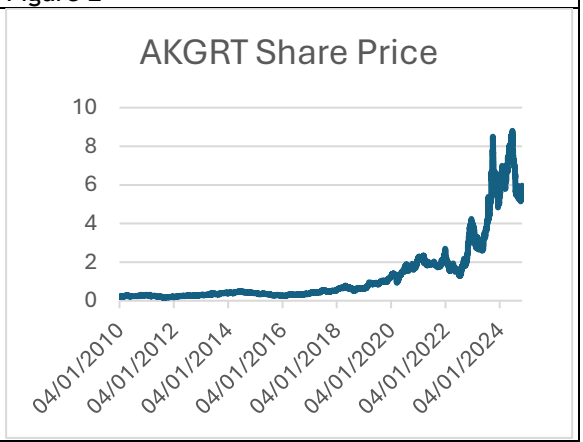


Figure 3

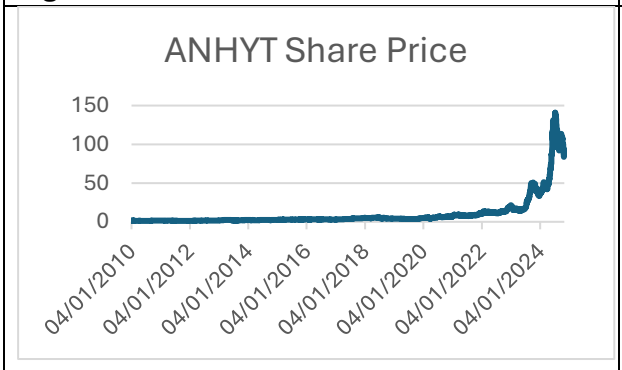


Figure 4

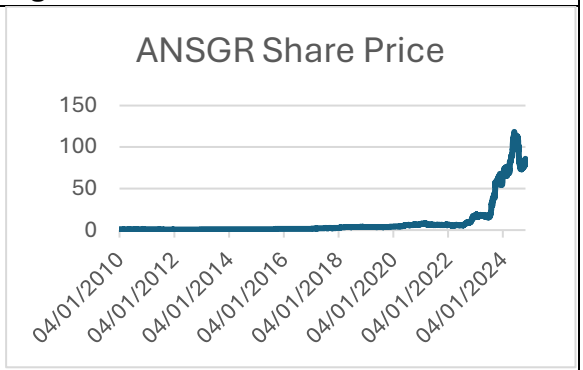


Figure 5

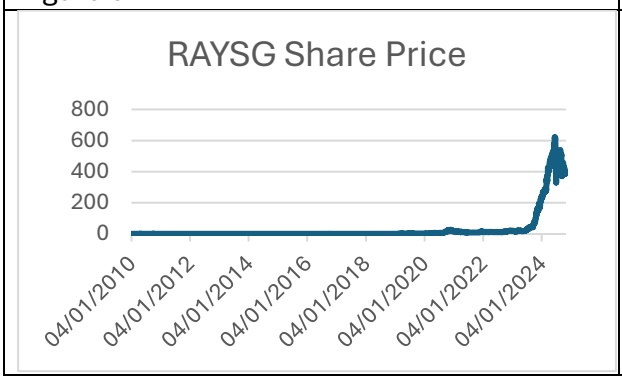
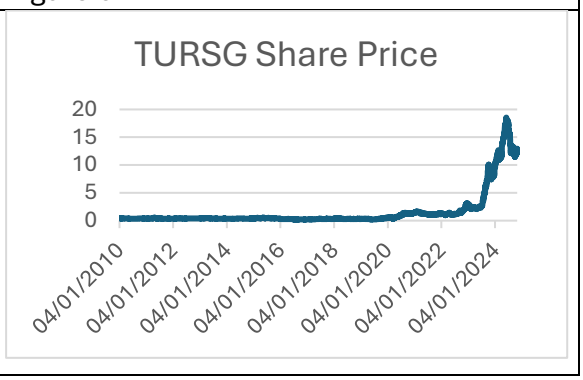


Figure 6



From Graph 1 to 6, there is historical data of our six selected insurance companies. These graphs show the prices and complete pattern of our selected insurance companies listed in BIST-100 over the years from 2010 to 2024. The share prices are escalating from 2010 to start of 2023 for companies (ANHYT, ANSGR, RAYSG and TURSG) and then increased drastically. Whereas for AKGRT and AGESA,

there are, fluctuation started from 2021 with increasing pattern. Therefore, the behavior of these selected companies are not the same, which makes them a good study case to analyze.

3.2. Techniques for Anomaly detection:

In this study, our aim is to develop such a methodology that will helps us to identify anomalies in the stock market data, for the purpose we use four different volatility measures that are directly measured from the data. As they are different in nature i.e, down to up volatility and relative frequency are measured as second-moment, capturing variations in market movements. In contrast, the Garman-Klass approach for risk is derived from daily data, providing results on daily basis. However, the NSK is calculated as third moment and capture the lower price fluctuations, provides insight into downside risk within financial market. After calculating the volatility measures, we used 95% confidence interval ($\cup \pm 2\delta$) to detect the anomalies from each measure. As our four volatility measures are different in nature, so they capture anomalies in different time span. In order to have robust and comprehensive results we find joint anomaly, where we used two different methods i) Z Score normalization and ii) Mahalanobis Distance. After calculating these two again, we have one variable each and to find the anomaly we again use 95% confidence interval ($\cup \pm 2\delta$). These measures explained as follows:

3.2.1. Techniques for volatility measures:

Four different volatility measures i.e, Negative conditional return skewness, Down to up volatility, GK approach for risk and Relative frequency are used and they measured by the following formulas:

a. Negative Conditional Return Skewness (NCRS): This captures the risk of negative changes in the prices and can inform market dips after a artificially inflated prices (Cao et al., 2013).

$$NCKEW_{it} = -\left[n(n-1)^{\frac{3}{2}}\sum W_{it}^{3}\right] / \left[(n-1)(n-2)(W_{it}^{2})^{3/2}\right]$$

Of course, when n is the number of trading days for firm i in quarter t. This also reveals that higher NCSKEW means higher crash risk (Chen et al., 2001).

b. Down-to-Up Volatility (DUV): Explaining this, it indicated that this metric is logical in showing us the degree of proportional change in prices and thus, the level of asymmetry that exists during manipulation (Leangarun et al., 2021).

$$DUVOL_{it} = \ln \frac{\{(n_u - 1)\sum_{down} W_{jt}^{2}\}}{(n_d - 1)\sum_{up} W_{jt}^{2}}$$

Where n_u is the number of "up" days and n_d is the number of "down" days for form I within quarter t. A high DUVOL suggests the highest fraud risk.

c. GK Approach for Risk (GK): A daily return variability-based risk estimator which provides view into heightened risk levels associated with fraud (Garman & Klass, 1980, Haykir & Yagli, 2022; Molnar, 2016)

$$EXV_t = \sqrt{\frac{1}{2}(eh_t - el_t)^2 - (2log2 - 1)ec_t^2}$$

eh_t = log ($high_t$) - log ($open_t$)
el_t= log (low_t) - log ($open_t$)
ec_t^2= log ($close_t$) - log ($open_t$)

d. Probability or Relative Frequency (RF): These measures make use of the fact that the return distributions in the case of manipulated data differ from those of normal stocks (Abbas et al., 2019; Piotroski, J. D., Wong, T. J., & Zhang, T. (2015).

3.2.2. Techniques for Joint Anomaly Detection:

After estimating the volatility measures to capture the anomalies in insurance sector of BIST-100 historical data set, now, we are going to find joint anomaly detection by using two different techniques. When we have four different results from different anomaly detection techniques (Risk Measures), then we need to have combined anomalies so it gives us easy and better understand for outliers / anomalies that we have to focus. We calculate Z score normalization and Mahalanobis distance and then calculate the Anomalies by using 95% confidence interval ($\cup \pm 2\delta$) and the values outside this will be considered as outliers/anomalies.

a. **Z Score Normalization:** when we have more than one variables and wants to find their joint effect and they have different measure. Then, we can calculate Z score by this formula for each variable:

$$\frac{(X - Min\ X)}{Max\ x - MinX}$$

Here x is the values of variable and from the same variable we can calculate minimum (Min X) and maximum values (Max X) (Jain, A., et al., 2005).

b. **Mahalanobis Distance:** This technique is also used to find joint relationship / effect of different variables, calculated for the same purpose. The Mahalanobis distance calculations can be find out as follows:

$$D^2 = (\frac{(Xi - U)}{\delta})^T \varepsilon^{-1} \frac{(Xi - U)}{\delta}$$

Here Xi is the value of each variable, U is the mean and δ is the variance. Then we have to take the transpose of this vector and multiply with the covariance matrix and matrix $\frac{(Xi-U)}{\delta}$ to find the Mahalanobis distance (Flores-Guerrero, J. L., et al., 2021).

1. Results and Discussion

This section is divided into three subsections, i.e. descriptive statistics, anomaly detection estimation and Joint anomaly detection.

1.1. Descriptive statistics

Table 1 presents the basic descriptive statistics. The average price value highlights the differences in share prices among the selected companies, while the standard deviation reflects the dispersion of the data. The coefficient of variation (CV) offers a measure of relative dispersion across all series. The data indicate that only two of the selected companies exhibit a lower relative dispersion compared to the CV of the overall market, whereas four companies demonstrate more volatile series than the broader market.

Table 1: number of observations, monthly average, minimum and maximum price and standard deviation for selected companies and BIST.

Company	Obs	Mean	Std. Dev.	CV	Min	Max
AGESA	2499	22.212	24.961	1.124	6.32	130.5
AKGRT	3722	1.312	1.73	1.319	0.145	8.8
ANHYT	3722	9.991	20.172	2.019	0.96	140.8
ANSGR	3722	9.351	20.757	2.22	0.553	118.3
RAYSG	3722	30.305	98.784	3.26	0.41	622
TURSG	3722	1.551	3.224	2.079	0.188	18.538
BIST100	3722	1879.469	2420.436	1.288	487.39	11172.75

1.2. Anomaly detection estimation

As described in the previous section, all four-risk measure methods were applied on the data set and calculate the values for these measures and then use 95% confidence interval ($\cup \pm 2\delta$) approach to detect the anomalies in RF, GK risk, Down to Up volatility and NCSK for the selected insurance companies.

From Figure 7, 8, 9 and 10 for the first company, AGESA, the Down-to-Up Volatility method estimated 6 anomalies, NCRS detected 7, Relative Frequency method detected 3 and GK approach detected one anomaly.

Figure 7

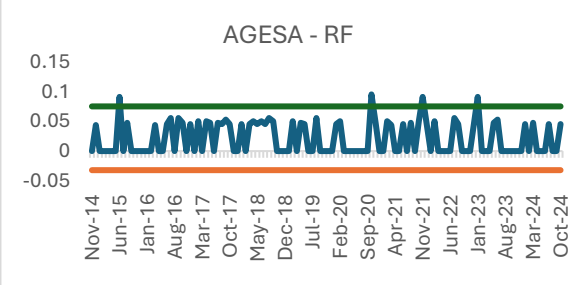


Figure 8

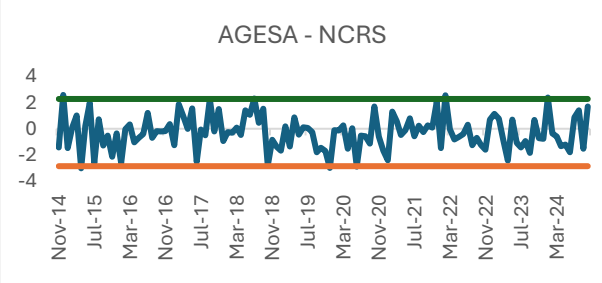


Figure 9

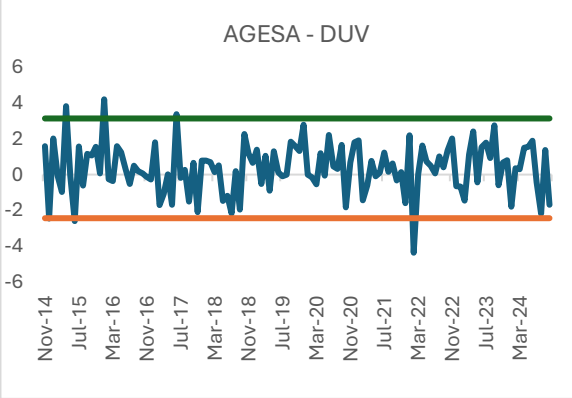
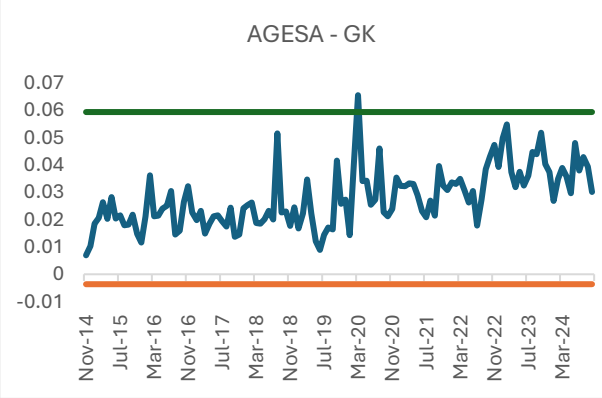


Figure 10



Similarly, for AKGRT company, the Down-to-Up Volatility method estimated 11 anomalies, NCRS detected 10, Relative Frequency method detected 10 and GK approach detected 11 anomalies, as presented in the below figures (11-14).

Figure 11

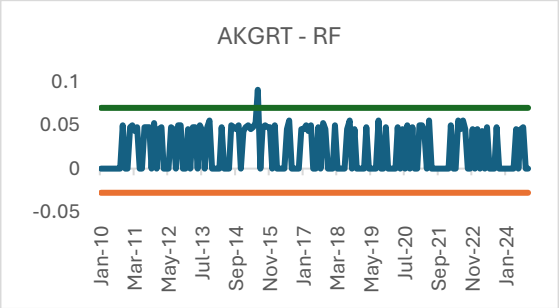


Figure 12

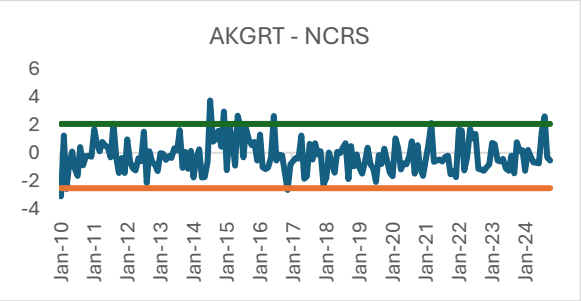


Figure 13

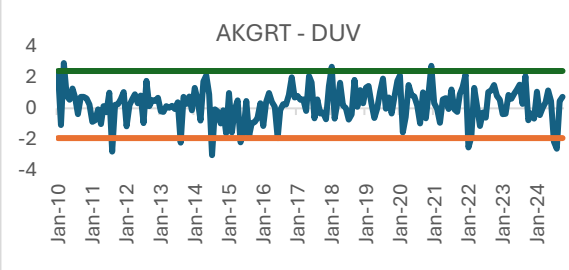
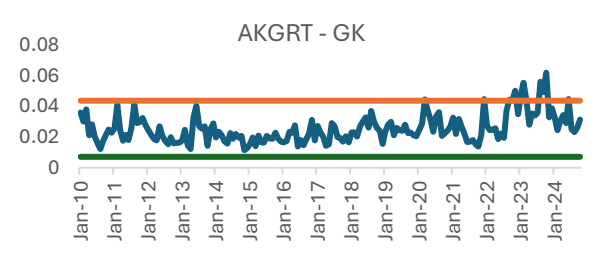


Figure 14



Furthermore, for ANHYT company, the Down-to-Up Volatility method estimated 10 anomalies, NCRS detected 8, Relative Frequency method detected 7 and GK approach detected 9 anomalies, as presented in the below figures (15-18).

Figure 15

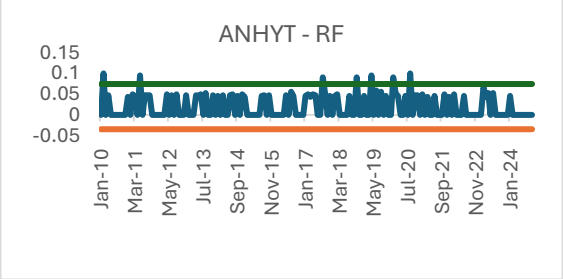


Figure 16

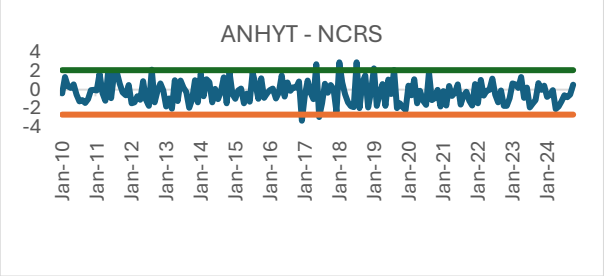


Figure 17

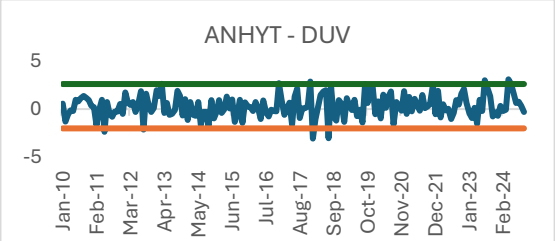
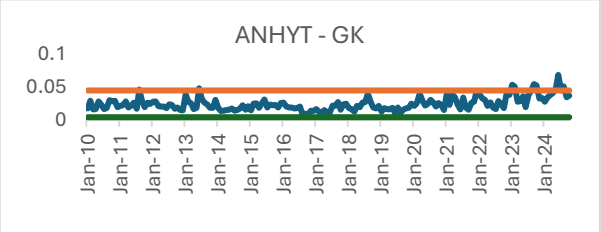


Figure 18



On similar lines, for ANSGR company, the Down-to-Up Volatility method estimated 10 anomalies, NCRS detected 8, Relative Frequency method detected 6 and GK approach detected 8 anomalies, as presented in the below figures (19-22).

Figure 19

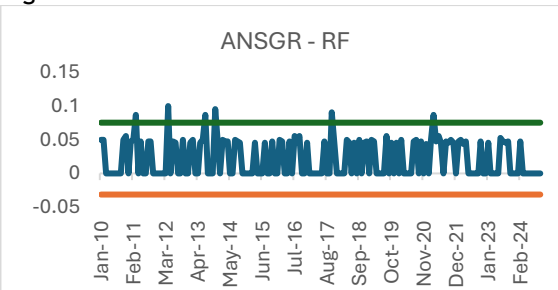


Figure 20

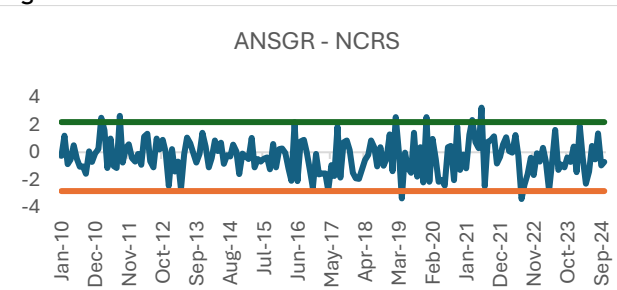


Figure 21

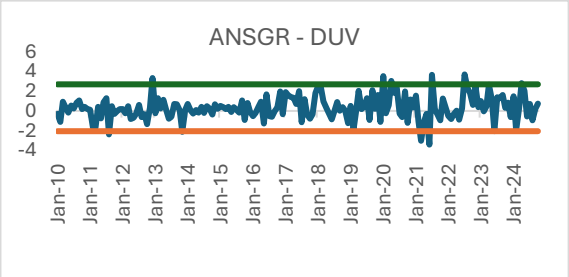
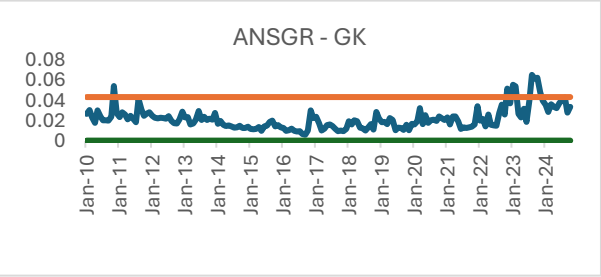


Figure 22



For RAYSG company, the Down-to-Up Volatility method estimated 9 anomalies, NCRS detected 9, Relative Frequency method detected 7and GK approach detected 13 anomalies, as presented in the below figures (23-26).

Figure 23

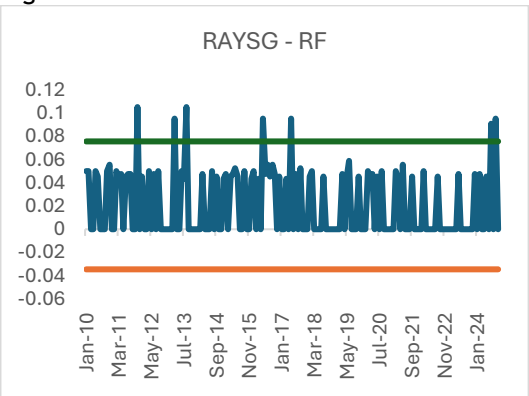


Figure 24

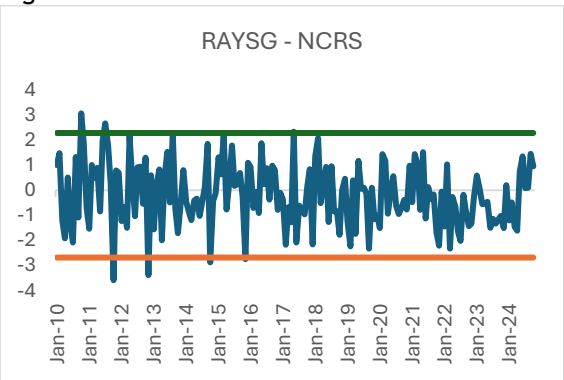


Figure 25

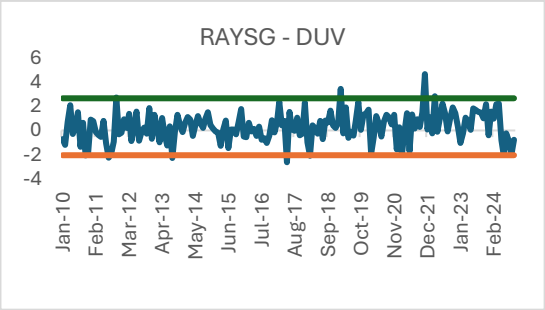
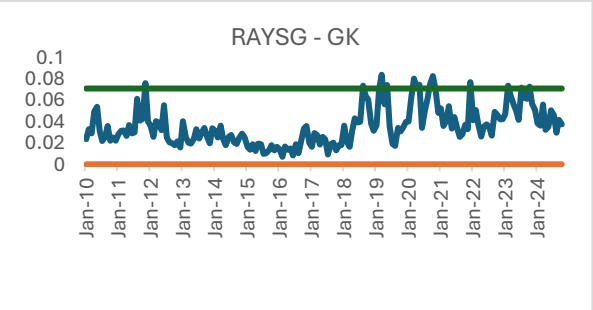


Figure 26



And lastly, for TURSG company, the Down-to-Up Volatility method estimated 7 anomalies, NCRS detected 7, Relative Frequency method detected 5 and GK approach detected 11 anomalies, as presented in the below figures (27-30).

Figure 27

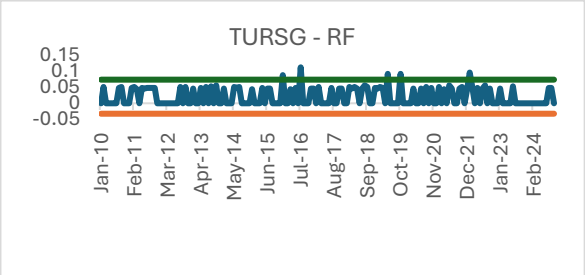


Figure 28

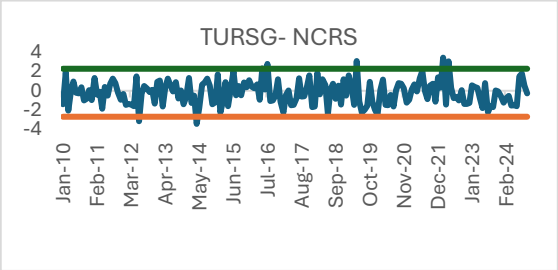


Figure 29

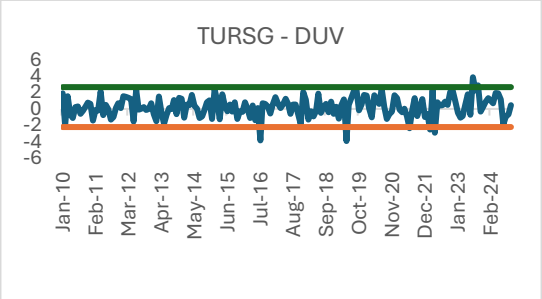
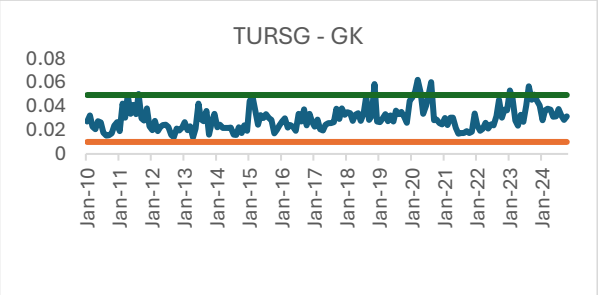


Figure 30



The analysis reveals inconsistencies among the four methods, with variations not only in the number of anomalies identified within a given period but also in their timing and direction. These discrepancies are further illustrated in the table below, which shows no correlation between GK and RF or GK and NSK, and only a weak correlation between GK and DUV. In contrast, DUV demonstrates a significant but negative correlation with RF and NCRS, while NCRS and RF exhibit a positive correlation.

Table 2: Correlation among the anomaly's detection methods

Variables	(1)	(2)	(3)	(4)
(1) RF	1.000			
(2) NCRS	0.574	1.000		
(3) DUV	-0.541	-0.913	1.000	
(4) GK	-0.075	-0.069	0.117	1.000

The highlighted results underscore the necessity of a comprehensive analysis of the predictors of the anomaly measure, which is presented in the following subsection.

1.3. Joint Anomaly Detection Methods

In order to have a joint Anomaly detection, we use two different techniques, i) Z Score Normalization and ii) Mahalanobis Distance. After calculating Z score for each risk measure, we take the average of it and then calculate the Anomalies by using 95% confidence interval ($\cup \pm 2\delta$) and the values outside this will be considered as outliers/anomalies. For Mahalanobis Distance, we consider Four Risk Measures (DUV, NSK, RF and GK) as vector and then use the distance formula$(\frac{(X-U)}{\delta})^T \varepsilon^{-1} \frac{(X-U)}{\delta}$, which is second moment and then calculate the Anomalies by using 95% confidence interval ($\cup \pm 2\delta$).

Figure 31

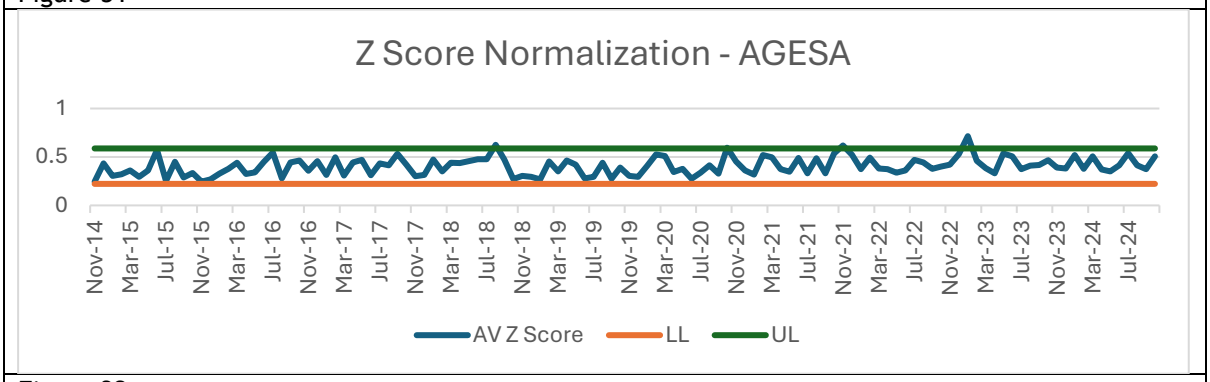
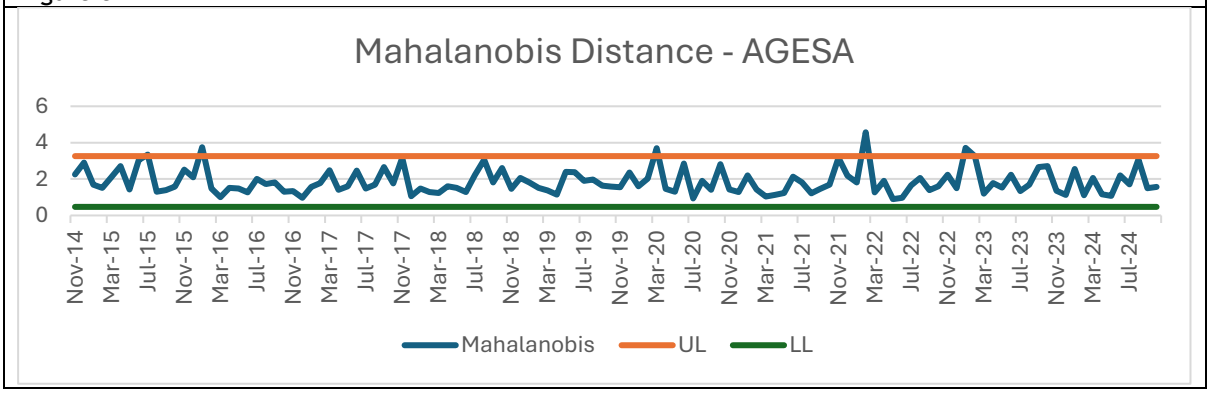


Figure 32



When we apply joint anomaly detection methods to find anomalies (Figure 31 and 32), we 4 anomalies in AGESA insurance company by Z score normalization whereas 5 anomalies by using Mahalanobis distance. Only the have one anomaly on the same time but when we investigated further the price of shares in selected anomalies months, it is revealed that Mahalanobis distance results are more accurate.

Figure 33

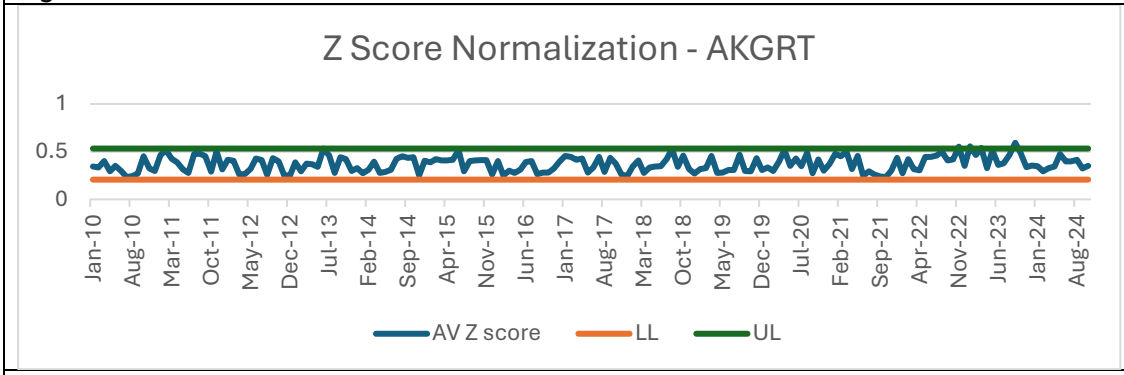
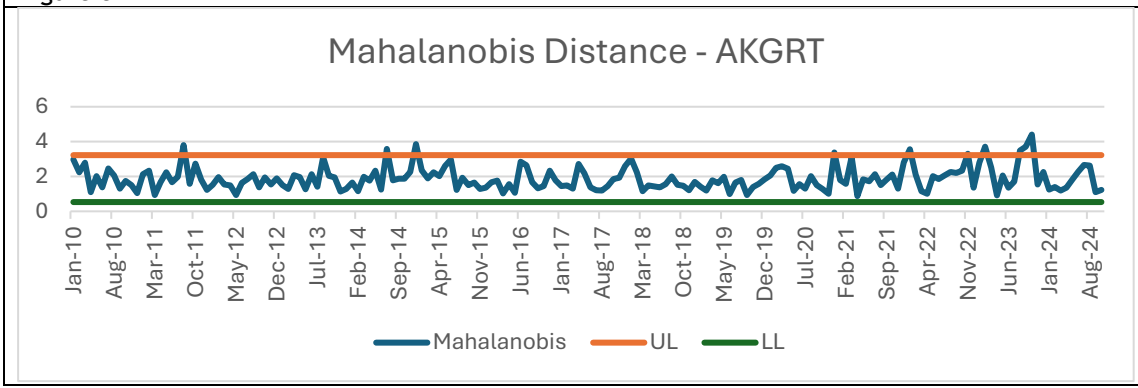


Figure 34



Similarly, the number of anomalies in AKGRT insurance company are 4 by using Z Score normalization whereas 10 by using Mahalanobis distance and in this insurance company, 2 anomalies are same by using different joint anomaly measure. Mahalanobis distance gives better results here as well.

Figure 35

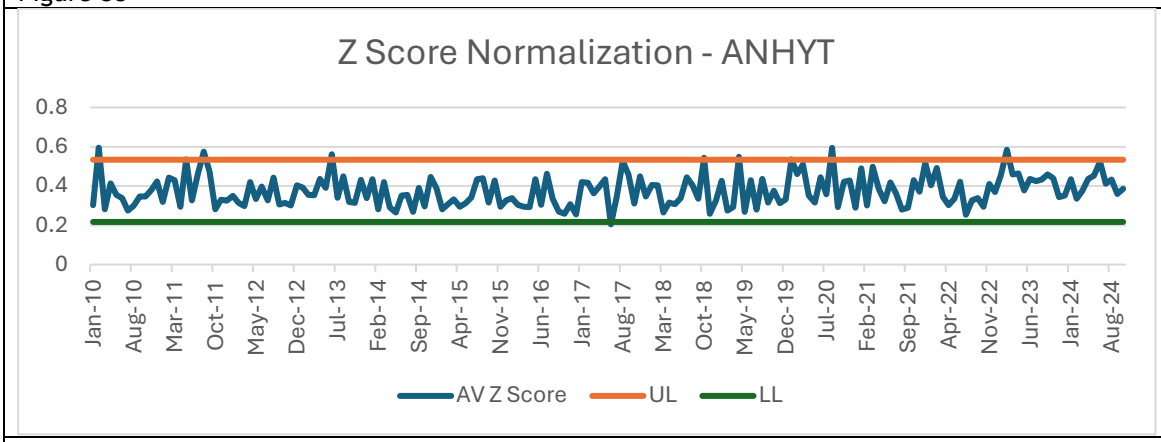
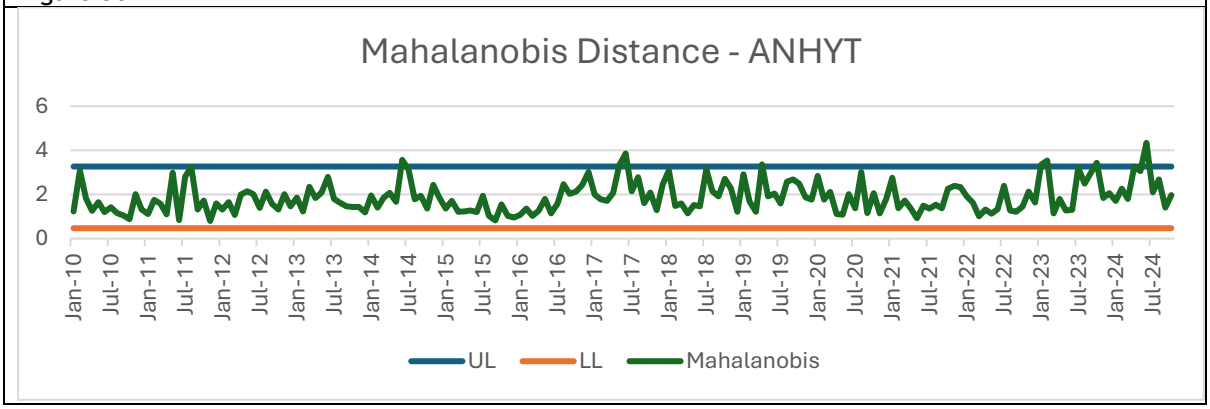


Figure 36



In Figure 35 and 36, Mahalanobis distance shows 08 anomalies whereas Z score normalization came with 10 anomalies and 03 of them are similar. Even number of anomalies are lesser by using Mahalanobis distance but the original data reveals that these 08 are real anomalies as compared to 10 by Z score.

Figure 37

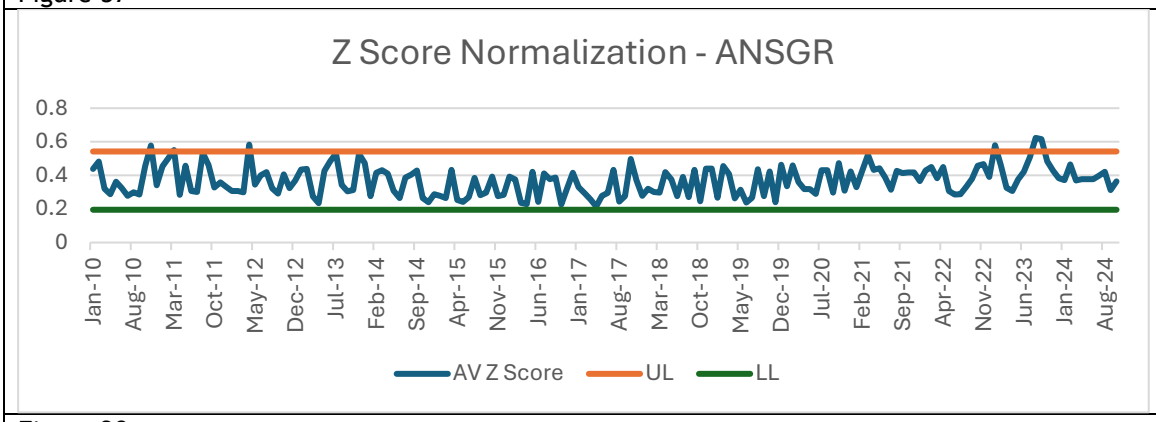
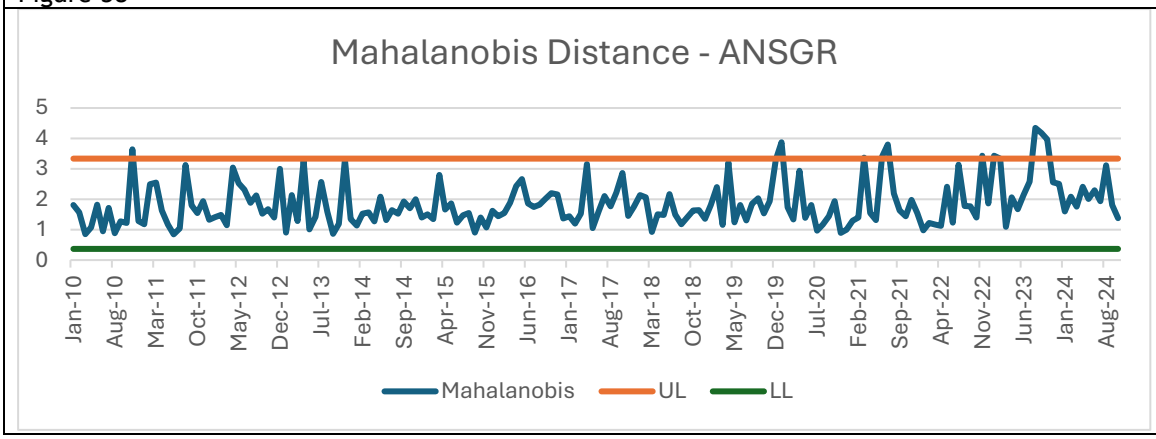


Figure 38



In figure 37 and 38, Z score normalization identify 06 anomalies in ANSGR insurance company where as Mahalanobis Distance detect 10 anomalies and out of them 4 anomalies are same (detected by both methods). Again, when we referred to the data, Mahalanobis distance performed well as compared to Z score normalization.

Figure 39

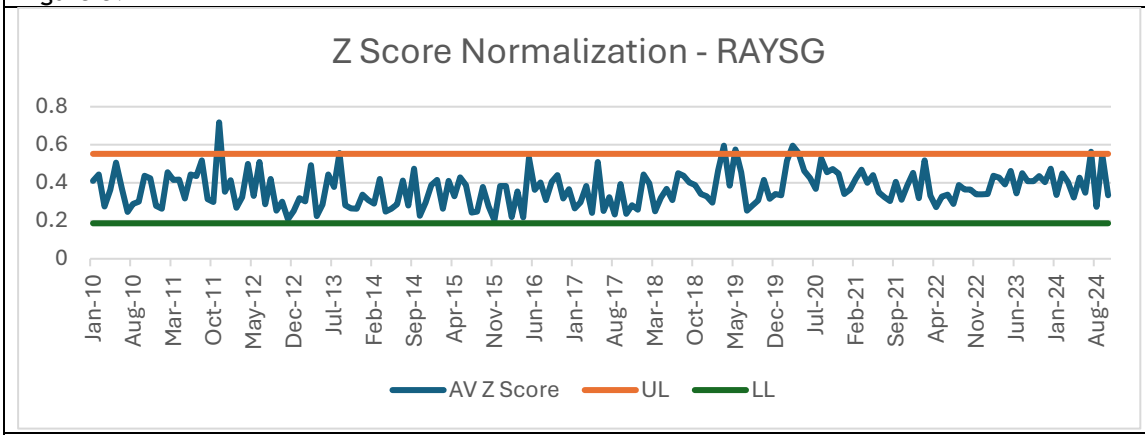
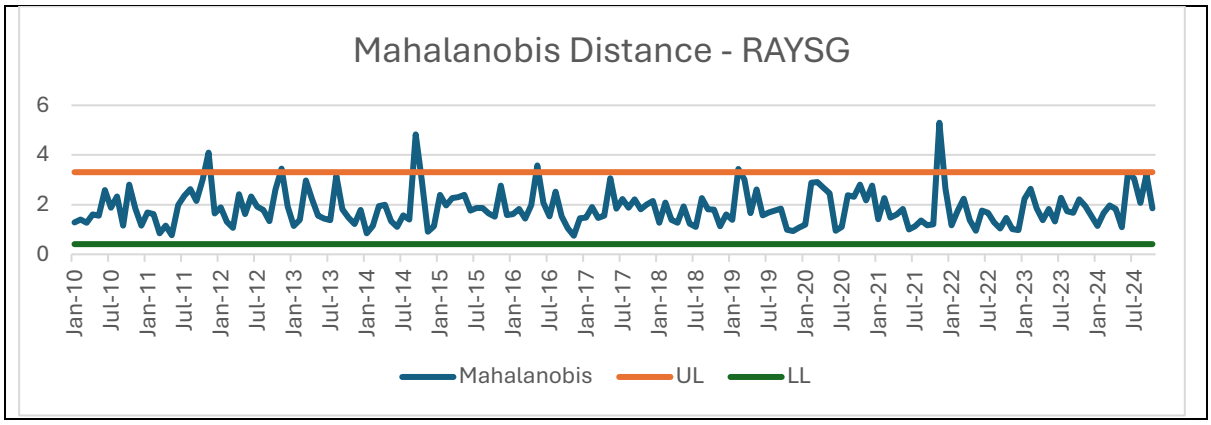


Figure 40



For RAYSG, Z Score Normalization detect 07 anomalies and Mahalanobis detect 06 anomalies but one anomaly is joint from the total anomalies they found. In term of RAYSG insurance, all 12 anomalies are important but Mahalanobis distance gave the best one.

Figure 41

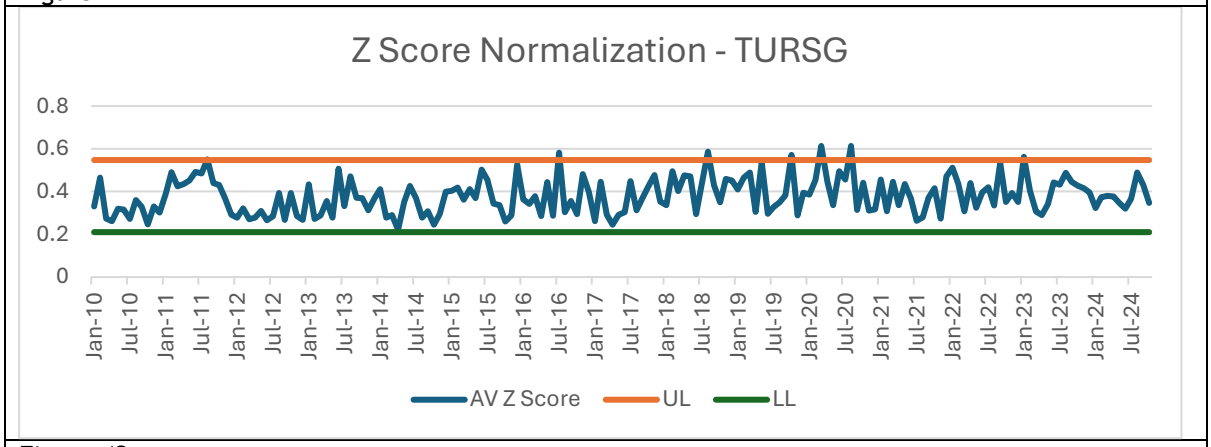
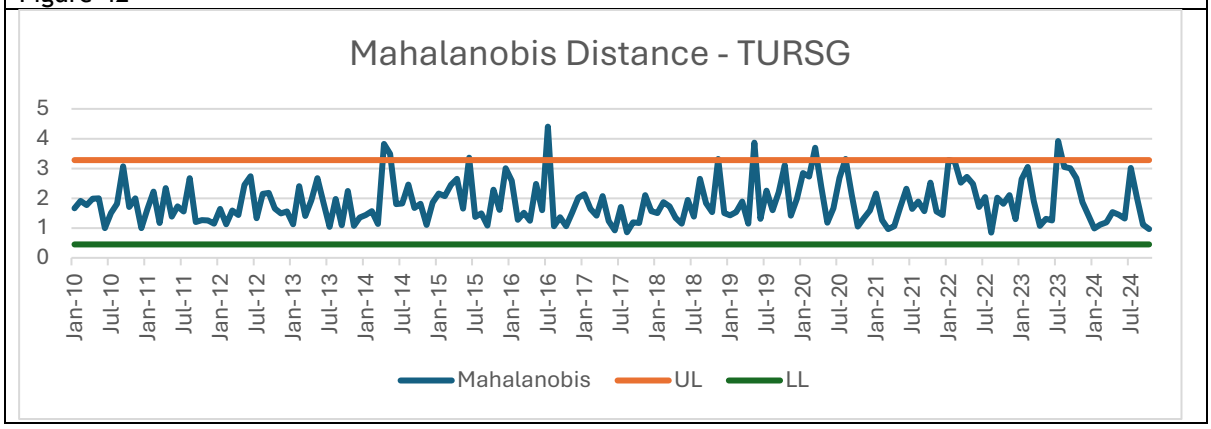


Figure 42



From figure 41 & 42, total 15 anomalies were detected from TURSG insurance company historical data. Through Mahalanobis Distance, 10 anomalies were detected, whereas, Z score normalization can detect 07 anomalies and overall 02 anomalies are same from the both methods.

2. Conclusion:

Our study is aimed to detect anomalies in the six listed insurance companies in Borsa-Istanbul using four different measures of risk. These measures of risk perform better as compared to the traditional model based anomaly detection methods (ARCH, GARCH, ARIMA) for financial fraud in Stock Exchange historical data. Because our measures of risk use the historical data directly for anomaly detection instead of making them, stationary and they do not need the data to follow the any distribution, so we can avoid the misspecification problem. Furthermore, it also gives the liberty from induced volatility, which comes from the mean equation of traditional anomaly detection methods. By using these measures of risk, we find that DUV perform well for AKGRT, AGESA and ANSGR whereas GK

approach provide better results by using data of ANHYT, RAYSG and TURSG as there is more volatility in their daily price. Overall, for AKGRT dataset all four measures of risk perform well.

As we have, different anomalies while using different measures of risk. Therefore, we develop a joint anomaly detection method, which is multi-dimensional and robust. For this reason, we use Z Score Normalization and Mahalanobis Distance approach. Z Score Normalization treat each measure equally as well as it ignores the overlapping effect among our anomaly detection measures. On the other hand, Mahalanobis distance method not only join them but also considers correlations among anomaly detection methods. The Results also provides the evidence that Mahalanobis distance perform well for joint anomaly detection, as it provides more anomalies as compared to Z Score Normalization and have some same anomalies. However, only for RAYSG the Z score Normalization perform well as compared to Mahalanobis distance.

Based on our conclusions, it is suggested that while doing anomaly detection in high frequency dataset, it is better to use these measures of risk rather than GARCH, ARIMA and ARMA models. Moreover, to have more comprehensive and robust results, one may use Mahalanobis distance and Z score normalization based on these four measures of risk. In future, the fraud detection through anomalies using these four risk measures and then on the basis of these four, the two robust measures can be used in cryptocurrency market as this market is highly volatile and prone to financial frauds.

3. References:

Abdulrhman, Alqurayn., Nada, Kulendran., Ranjith, Ihalanayake. (2024). 1. An event study of potential insider trading in the Saudi stock market. Cogent economics & finance, doi: 10.1080/23322039.2024.2367368

Abdul-Rahman, M., Khan, A.I., Kaplan, M., (2024). 1. Beyond GARCH: Intraday Insights Into the Exchange Rate and Stock PriceVolatility Dynamics in Borsa Istanbul Sectors. FWU journal of social sciences, doi: 10.51709/19951272/fall2024/1

Aggarwal, R. K., & Wu, G. (2006). Stock market manipulations. *The Journal of Business*, *79*(4), 1915-1953.

Ameyaw, M. N., Idemudia, C., & Iyelolu, T. V. (2024). Financial compliance as a pillar of corporate integrity: A thorough analysis of fraud prevention. Finance & Accounting Research Journal, 6(7), 1157-1177.

Brennan, N. M., & McGrath, M. (2007). Financial statement fraud: Some lessons from US and European case studies. Australian accounting review, 17(42), 49-61.

Brockman, P., Li, X., & Price, S. M. (2017). Conference call tone and stock returns: Evidence from the Stock Exchange of Hong Kong. *Asia-Pacific Journal of Financial Studies*, *46*(5), 667-685.

Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. *ACM computing surveys (CSUR)*, *41*(3), 1-58.

Chen, J., Hong, H., & Stein, J. C. (2001). Forecasting crashes: Trading volume, past returns, and conditional skewness in stock prices. Journal of financial Economics, 61(3), 345-381.

Comerton-Forde, C., & Putniņš, T. J. (2014). Stock price manipulation: Prevalence and determinants. *Review of Finance*, *18*(1), 23-66.

Dechow, P., Ge, W., & Schrand, C. (2010). Understanding earnings quality: A review of the proxies, their determinants and their consequences. *Journal of accounting and economics*, *50*(2-3), 344-401.

Fahlevie, R. A., Oktasari, E., Nurmawati, B., Setiawan, P. A. H., & Dimalouw, J. A. (2022). PUMP AND DUMP CRIMINAL OVERVIEW ACCORDING TO CAPITAL MARKET LAW NO. 8 YEAR 1995. Awang Long Law Review, 5(1), 167-179.

Flores-Guerrero, J. L., Grzegorczyk, M. A., Connelly, M. A., Garcia, E., Navis, G., Dullaart, R. P., & Bakker, S. J. (2021). Mahalanobis distance, a novel statistical proxy of homeostasis loss is longitudinally associated with risk of type 2 diabetes. *EBioMedicine*, *71*.

Fu, K., Cheng, D., Tu, Y., & Zhang, L. (2016). Credit Card Fraud Detection Using Convolutional Neural Networks. 13th Conference on Neural Information Processing Systems. Barcelona, Spain.

Garman, M. B., & Klass, M. J. (1980). On the estimation of security price volatilities from historical data. *Journal of business*, 67-78.

Groll, A., Khanna, A., & Zeldin, L. (2024). A Machine Learning-based Anomaly Detection Framework in Life Insurance Contracts. arXiv preprint arXiv:2411.17495.

Harvey, C. R., & Siddique, A. (2000). Conditional skewness in asset pricing tests. *The Journal of finance*, *55*(3), 1263-1295.

Hawkins, D. M. (1980). Identification of outliers. Heidelberg, Germany: Springer.

Haykir, O., & Yagli, I. (2022). Speculative bubbles and herding in cryptocurrencies. Financial innovation, 8(1), 78.

He, H., Wang, J., Graco, W., & Hawkins, S. (1997). Application of neural networks to detection of medical fraud. Expert Systems with Applications, 13(4), 329–336.

Heryadi, Y., & Warnars, H. L. (2017). Learning temporal representation of transaction amount for fraudulent transaction recognition using CNN, Stacked LSTM, and CNNLSTM. IEEE International Conference on Cybernetics and Computational Intelligence. Phuket, Thailand.

Hodge, V. J., & Austin, J. (2004). A survey of outlier detection methodologies. Artificial Intelligence Review, 22(2), 85–126.

Jain, A., Nandakumar, K., & Ross, A. (2005). Score normalization in multimodal biometric systems. *Pattern recognition*, *38*(12), 2270-2285.

Jurgovsky, J., Granitzer, M., Ziegler, K., Calabretto, S., Portier, P.-E., He-Guelton, L., & Caelen, O. (2018). Sequence classification for credit-card fraud detection. Expert Systems with Applications, 100, 234–245.

Kamini, Pareek., Renu, Sharma. (2023). 3. Machine Learning In Fraud Detection and Prevention. doi: 10.52783/tjjpt.v43.i3.2344

La Morgia, M., Mei, A., Sassi, F., & Stefa, J. (2023). The doge of wall street: Analysis and detection of pump and dump cryptocurrency manipulations. ACM Transactions on Internet Technology, 23(1), 1-28.

Lee, E. J., Lee, Y. K., & Kim, R. (2023). Profitability and herding of trade-based pump-and-dump manipulation. Applied Economics, 56(20), 2375–2385. https://doi.org/10.1080/00036846.2023.2182405

Li, Y., & Zhang, X. (2023). Daily Semiparametric GARCH Model Estimation Using Intraday High-Frequency Data. Symmetry, 15(4), 908. https://doi.org/10.3390/sym15040908

Lokanan, M., Tran, V., & Vuong, N. H. (2019). Detecting anomalies in financial statements using machine learning algorithm: The case of Vietnamese listed firms. Asian Journal of Accounting Research, 4(2), 181-201.

Luo, Y., & Zhang, C. (2020). Economic policy uncertainty and stock price crash risk. Research in International Business and Finance, 51, 101112.

Mandelbrot, B. (1963). New methods in statistical economics. Journal of political economy, 71(5), 421-440.

Palacio, S. M. (2019). Abnormal pattern prediction: Detecting fraudulent insurance property claims with semi-supervised machine-learning. Data Science Journal, 18, 35-35.

Piotroski, J. D., Wong, T. J., & Zhang, T. (2015). Political incentives to suppress negative information: Evidence from Chinese listed firms. Journal of Accounting Research, 53(2), 405-459.

Rozeff, M. S., & Zaman, M. A. (1998). Overreaction and insider trading: Evidence from growth and value portfolios. The Journal of Finance, 53(2), 701-716.

Senvar, O., & Hamal, S. (2022). Examining Fraudulent Financial Statements of Turkish Small and Medium Enterprises (SMEs) from Different Sectors. Avrupa Bilim ve Teknoloji Dergisi, (41), 211-220.

Seyhun, H. N. (1986). Insiders' profits, costs of trading, and market efficiency. *Journal of financial Economics*, *16*(2), 189-212.

Sundarkumar, G. G., & Ravi, V. (2015). A novel hybrid undersampling method for mining unbalanced datasets in banking and insurance. Engineering Applications of Artificial Intelligence, 37, 368–377.

Sundarkumar, G. G., Ravi, V., & Siddeshwar, V. (2015). One-class support vector machine based undersampling: Application to churn prediction and insurance fraud detection. IEEE International Conference on Computational Intelligence and Computing Research. Madurai, India.

Svitlana, Y., & Kostiantyn, H. (2023). World stock market: Current state and prospects of development of stock exchange. Ekon. Vìsnik Dnìprovs'kogo Deržavnogo Teh. Unìversitetu, 2, 60-66.

Tao, H., Zhixin, L., & Xiaodong, S. (2012). Insurance Fraud Identification Research Based on Fuzzy Support Vector Machine with Dual Membership. International Conference on Information Management, Innovation Management and Industrial Engineering. Sanya, China.

Viaene, S., Dedene, G., & Derrig, R. A. (2005). Auto claim fraud detection using Bayesian learning neural networks. Expert Systems with Applications, 29(3), 653–666.

Wang, Y., & Xu, W. (2018). Leveraging deep learning with LDA-based text analytics to detect automobile insurance fraud. Decision Support Systems, 105, 87–95.

Wells, J. T. (2017). *Corporate fraud handbook: Prevention and detection*. John Wiley & Sons.
Wiese, B., & Omlin, C. (2009). Credit Card Transactions, Fraud Detection, and Machine Learning: Modelling Time Series with LSTM Recurrent Neural Networks. In Innovations in Neural Information Paradigms and Applications (pp. 231–268). Heidelberg, Germany: Springer.

Xu, Z., Li, X., Chevapatrakul, T., & Gao, N. (2022). Default risk, macroeconomic conditions, and the market skewness risk premium. Journal of International Money and Finance, 127, 102683.

Zhang, M., Li, T., Yu, Y., Li, Y., Hui, P., & Zheng, Y. (2020). Urban anomaly analytics: Description, detection, and prediction. *IEEE Transactions on Big Data*, *8*(3), 809-826.