FWU Journal of Social Sciences, Summer 2025, Vol.19, No.2, 59-72
DOI: http://doi.org/10.51709/19951272/Summer2025/5

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

Muhammad Nouman Latif, Muhittin Kaplan and Asad Ul Islam Khan
Ibn Haldun University, Istanbul, Turkiye

This study aims to identify anomalies in the financial data of six leading insurance companies listed on Borsa Istanbul, Türkiye. Traditional anomaly detection methods like GARCH, ARIMA and moving averages have inherent limitations, including the requirement of stationarity, strict distributional assumptions and risks of model mis-specification. To address these issues, we employ four alternative risk measures, i.e., Down-to-Up Volatility (DUV), Negative Conditional Skewness (NCS), Relative Frequency (RF) and the Garman-Klass (GK) on daily stock price data, thereby avoiding stationarity and distribution-related constraints. Our findings reveal significant differences in anomaly detection across these measures. While DUV and RF, which are based on second-moment calculations, capture variations in volatility, the GK approach (computed daily) and the NCS, which considers third-moment characteristics, provide complementary insight. To enhance robustness, we apply both Z-score normalization and Mahalanobis distance for joint anomaly detection. The Z-score method treats all risk measures equally and is suitable for normally distributed data but overlooks potential correlations. In contrast, Mahalanobis distance accounts for multivariate anomalies and interdependencies between risk measures, offering a more holistic approach. Our results indicate that Mahalanobis distance outperforms Z-Score normalization in detecting anomalies in five out of six insurance companies, except in the case of RAYSG. This study underscores the importance of alternative risk measures and multivariate anomaly detection techniques in financial fraud analysis, offering valuable insights for risk management and regulatory practices in emerging financial markets .

***Keywords*:** anomaly detection, financial fraud, risk measures, emerging insurance market.
JEL Classification: C58; C63; G22; G32

Financial fraud remains 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 a resilient financial system that facilitates 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 savers. These financial systems include market-based, bank-based, digital, and decentralized frameworks. Each plays a crucial role in maintaining financial stability and promoting economic growth. Among the four financial systems mentioned above, the market-based system is the most dominant (Svitlana & Kostiantyn, 2023). Within this system, stock markets, bonds market and foreign exchange rate markets serve as critical components. Among these, stock markets play a particularly crucial role due to their inherently volatile nature (Khan et al., 2024). 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 decisions, ensuring market stability and enhancing fraud detection mechanisms.

Correspondence concerning this article should be addressed to Muhammad Nouman Latif, PhD Candidate, Department of Economics, School of Business, Ibn Haldun University, Istanbul, Turkiye (Email id: muhammad.latif@stu.ihu.edu.tr

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. First, the infamous pump and dump schemes typify market manipulation, wherein a group of traders hypes up a stock to inflate its price before selling it off, leaving other investors to face subsequent price drops (La Morgia et al., 2023; Lee et al., 2024). The second type of manipulation includes creating false market conditions through practices such as wash trading or spoofing, where traders place orders with the intent to deceive others about stock demand (Comerton-Forde & Putniņš, 2014). Third, insider trading occurs when those with privileged information about a company's future performance or strategic plans 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 effectively identify and deter such actions (Alqurayn et al., 2024; Seyhun, 1986). Lastly, accounting fraud occurs when individuals alter a company's financial records, often by falsifying information about earnings or asset growth.

These fraudulent practices have serious consequences, often leading to significant stock mispricing and harming uninformed investors. For instance, the Enron and WorldCom cases underscore the risks of unregulated accounting manipulations and the need for strict fraud detection procedures (Dechow et al., 2010). Therefore, detecting financial fraud is critical to maintaining the integrity of financial markets. Fraudulent activities weaken investor confidence and mislead market dynamics, which can result in financial loss for both investors and the companies. If left undetected, these activities can harm stakeholders and 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 faults 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 fraudulent activities can be observed through anomalies or unusual patterns in financial data (Chandola et al., 2009; Hawkins, 1980; Faizan et al., 2018). One widely used approach to detect financial fraud is involves anomaly detection methods. These methods aim to identify irregular patterns in financial data that may signify fraudulent activity. Anomaly detection has been used in various domains including finance to uncover suspicious transactions, manipulative trading or misreported financial information (Fahlevie et al., 2022; La Morgia et al., 2023).

The use of traditional statistical or model-based anomaly detection methods find limited mentions in the literature due to their limitations. A key limitation lies in their assumptions about the nature of data, such as normality or stationarity, which are often violated in financial datasets (Salas-Molina et al., 2017). These models, like ARCH and GARCH, designed to capture volatility patterns, usually struggle when applied to high frequency data (Chai et al., 2023; Teker et al., 2024). Moreover, general weakness of these methods includes their inability to detect false positives and limited efficiency when handling large datasets (Chai et al., 2023). To address 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 select insurance companies listed in Borsa-Istanbul. These measures of risk offer several advantages over traditional methods, as they are distribution free, contain no model assumption (linear/non-linear) and find volatility directly from data, thereby avoiding problems related to induce volatility.

This study applies four different risk measures to detect anomalies, each with a distinct approach and philosophy. First, Down-to-Up Volatility (DUV) which measures the variation in positive and negative returns in a month, is a measure of risk, representing the disparity between upward and downward price movements and has previously been useful in capturing abnormal price action that could be construed as fraudulent activities (Brockman et al., 2017). The second approach, also widely used is the GK measure of risk (captures the intra-day volatility), used to estimate total risk exposure in the portfolio or market or within a particular sector by specifying the extreme market conditions and potential anomaly, thereby aiding in fraud identification (Haykir & Yagli, 2022a). Both these techniques are based on risk or volatility and approximate 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., 2022). The third useful indicator is the Negative

Conditional Return Skewness (NCS) – 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 et al., 2022). The fourth measure is the Relative Frequency (RF) of crash days in a month. The third and fourth measures are used as crash risk measures in the literature (PIOTROSKI et al., 2015) and are approximations of the third moment of distribution. After estimating these four risk measures, this study seeks to provide a more comprehensive analysis by combining their effects using two techniques, the Z-score normalization (Jain et al., 2005) and the Mahalanobis distance (Flores-Guerrero et al., 2021) to find joint anomaly detection, then the results will be more robust and reliable.

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 (Hashim et al., 2020). 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 & Hamal, 2022). The need for identification of such activities is therefore paramount to upholding market integrity and preventing financiers and competitors from being defrauded. If fraud remains undetected, organizations often face increased financial losses, legal liabilities and damage to their reputation, ultimately causing the public to lose confidence in financial markets (Wells, 2017). Besides, it also reduces specific risks and prevents the recurrence of fraud, and further ensures compliance with financial regulations (Ameyaw et al., 2024). Consequently, both statistics and machine learning are now considered crucial in spotting fraudulent behavioral patterns and containing their impact (Pareek et al., 2022).

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. Discrepancies in trade volume, price, and financial statement disparity are suggestive of manipulative fraud such as market manipulation and insider trading, or financial statement fraud (Brennan & McGRATH, 2007; Brockman et al., 2017). Identifying these anomalies has proven essential in minimizing risks and maintaining specific standards (Zhang et al., 2022). For instance, insider trading causes price changes that differ from historical trends and should thus be flagged as Anomalies (Rozeff & Zaman, 1998). Likewise, fraudulent reporting of financial statements may affect some essential values, including earnings or revenue, which can be identified through anomaly detection (Lokanan et al., 2019).

Several scholars have argued that anomalies 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, as in the case of pump-and-dump schemes or even Ponzi schemes (Rozeff & Zaman, 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 et al., 2024). It is possible to mitigate fraud through a proactive approach, which benefits both financial institutions and regulators by providing real-time detection and preventive measures', increasing market efficiency and stability (Brockman et al., 2017). In other words, anomaly detection remains an essential component of contemporary fraudulent detection models as they can identify financial crimes that may otherwise go unnoticed (Lokanan et al., 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. A growing consensus in the literature suggests that anomaly detection serves as a proxy for financial fraud detection. However, the methods of identifying anomalies vary across studies, ranging from those based on AI and machine learning to traditional statistical methods. Based on this consensus in the literature, the present study also adopts anomaly detection as an indicator of financial fraud. Specifically, it applies four different methods of risk measures, rooted in traditional statistics for anomaly detection.

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

Method

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

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, the current study focuses only on 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.(AKGRT), Anadolu Hayat Emeklilik A.Ş. (ANHYT), Anadolu Anonim Türk Sigorta Şirketi (ANSGR), RAY sigorta A.Ş. (RAYSG), Türkiye Sigorta A.Ş.(TURSG) listed in Borsa Istanbul (BIST-100) have been used. The Y-axis represents share price in Turkish Lira while the X-axis shows dates.

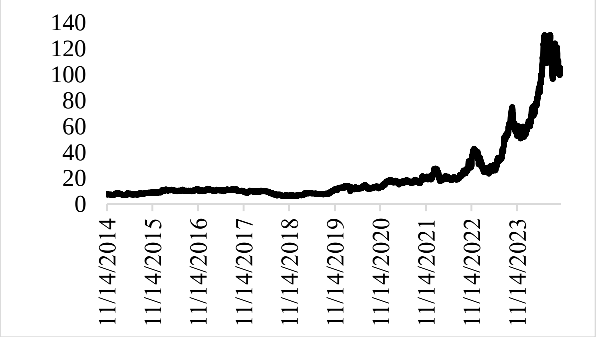


Figure 1: AGESA Share Price

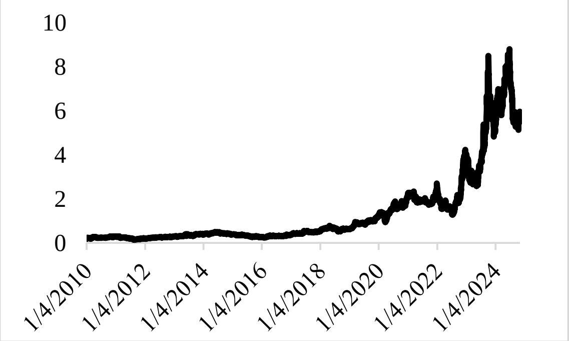


Figure 2: AKGRT Share Price

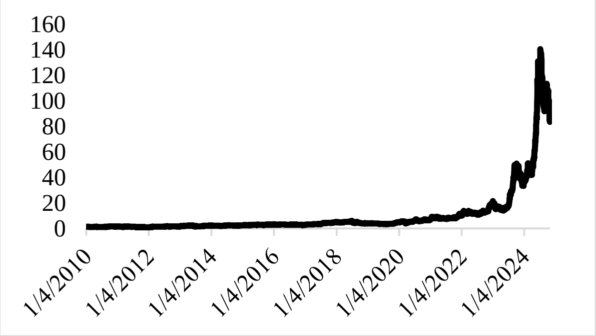


Figure 3: ANHYT Share Price

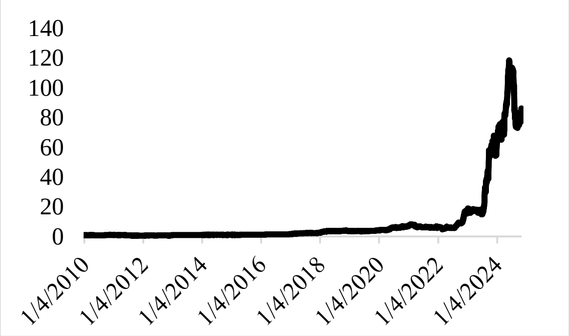


Figure 4: ANSGR Share Price

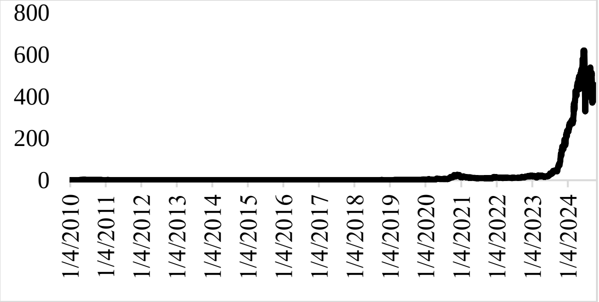


Figure 5: RAYSG Share Price

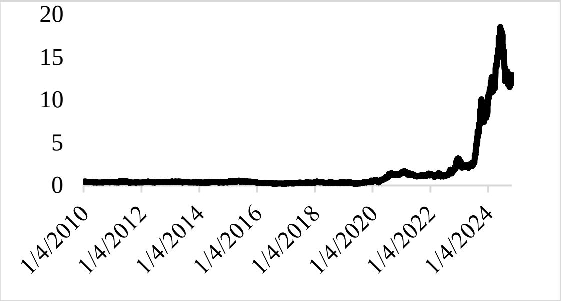


Figure 6: TURSG Share Price

Figures 1 to 6 display the historical data of the six selected insurance companies. These graphs show the prices and complete pattern of the 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, the fluctuation started from 2021 showing an increasing pattern. Therefore, the behavior of these selected companies is not the same, which makes them a good study case to analyze.

Techniques for Anomaly detection:

In this study, we develop a methodology that will help identify anomalies in stock market data. For this purpose, we used four different risk measures directly derived from the data, and which vary in nature. The Down-to-Up Volatility (DUV) and Relative Frequency (RF) are measured as second-moment, capturing variations in market movements. In contrast, the Garman-Klass (GK) approach for risk is derived from daily data, providing results on daily basis. However, the NCS 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 are explained as follows:

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 (NCS):** This captures the risk of negative changes in the prices and can inform market dips after artificially inflated prices (Chang et al., 2013).

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

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):** It is 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 (Chen et al., 2001).

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

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, 2022b).

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

$$eh_t = \log(high_t) - \log(open_t)$$

$$el_t = \log(low_t) - \log(open_t)$$

$$ec_t^2 = \log(close_t) - \log(open_t)$$

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 (PIOTROSKI et al., 2015).

1.1.1. Techniques for Joint Anomaly Detection:

After estimating the individual risk measures to capture anomalies in the insurance sector using the BIST-100 historical dataset, the next step involved conducting joint anomaly detection through 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 calculated Z-score normalization and Mahalanobis distance and then calculated 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 variable and want 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 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 et al., 2021).

Results and Discussion

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

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

Descriptive Statistics of Six Listed Insurance Companies Share Price

Company	Observations	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

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 NCS for the selected insurance companies. Due to their different nature, they detect anomalies sometimes at different time in the data-set.

Within Figures 7, 8, 9 and 10 regarding AGESA, the first company, the DUV method estimated six anomalies, NCS detected seven, RF method detected three and GK approach detected one anomaly. Notably, the month of June 2015 is a common anomaly across DUV, NCS and RF.

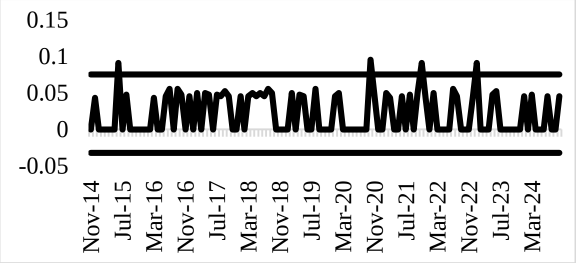


Figure 7: Anomalies in AGESA by using RF

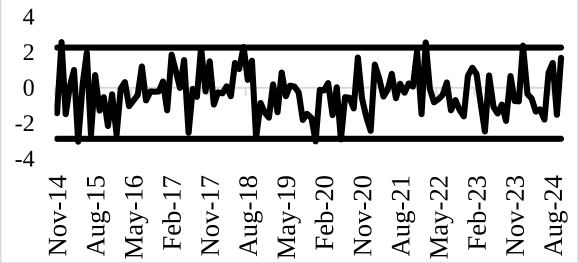


Figure 8: Anomalies in AGESA by using NCS

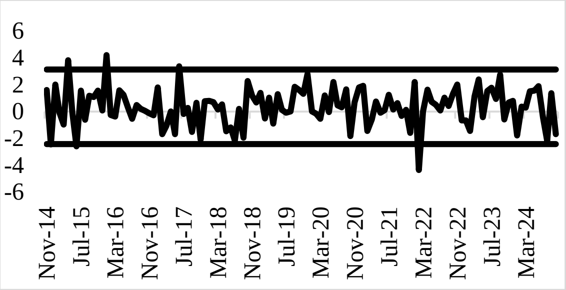


Figure 9: Anomalies in AGESA by using DUV

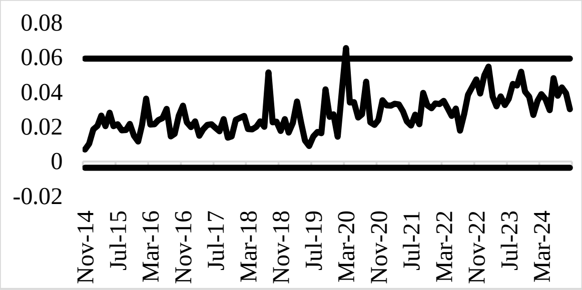


Figure 10: Anomalies in AGESA by using GK

Similarly, for AKGRT company, the DUV method estimated 11 anomalies, NCS detected 10, RF method detected 10 and GK approach detected 11 anomalies, as presented in the figures below (Figures 11-14).

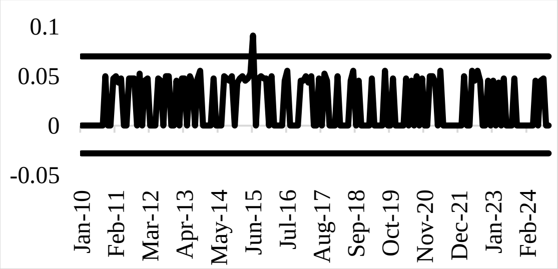


Figure 11: Anomalies in AKGRT by using RF

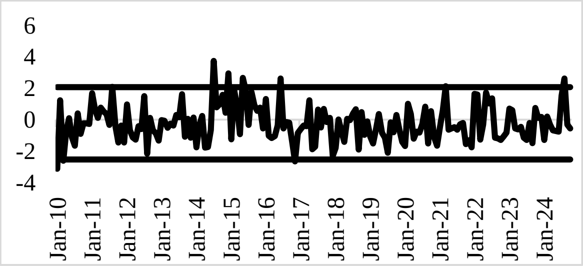


Figure 12: Anomalies in AKGRT by using NCS

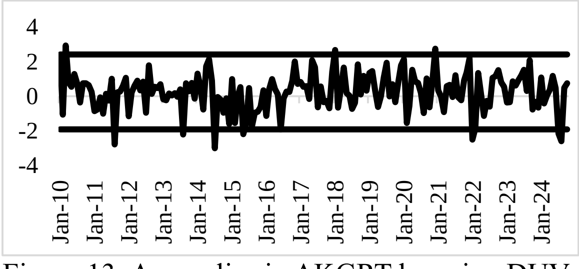


Figure 13: Anomalies in AKGRT by using DUV

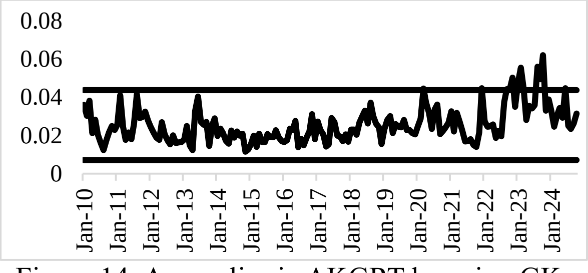


Figure 14: Anomalies in AKGRT by using GK

Furthermore, for ANHYT company, the DUV method estimated 10 anomalies, NCS detected eight, RF method detected seven and GK approach detected nine anomalies, as presented in the figures below (Figures 15-18).

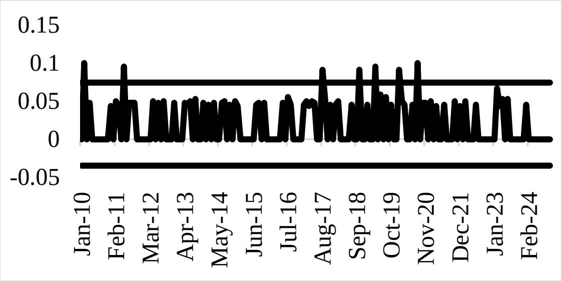


Figure 15: Anomalies in ANHYT by using RF

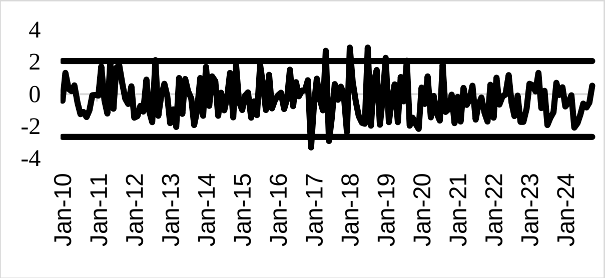


Figure 16: Anomalies in ANHYT by using NCS

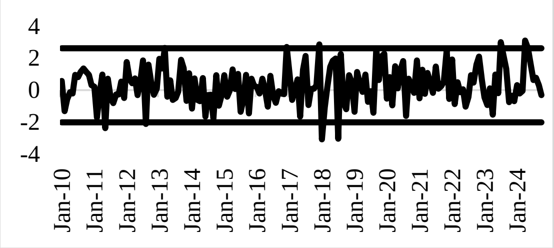


Figure 17: Anomalies in ANHYT by using DUV

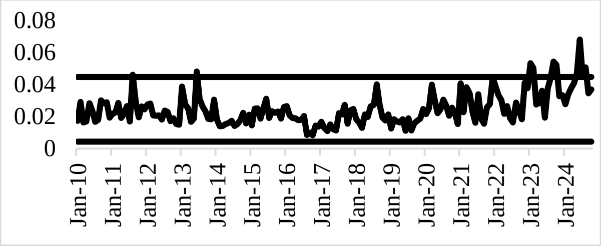


Figure 18: Anomalies in ANHYT by using GK

On similar lines, for ANSGR company, the DUV method estimated 10 anomalies, NCS detected eight, RF method detected six and GK approach detected eight anomalies, as presented in the figures below (Figures 19-22).

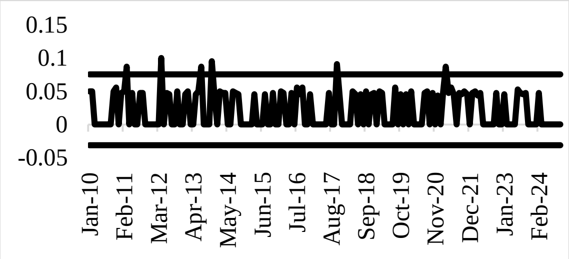


Figure 19: Anomalies in ANSGR by using RF

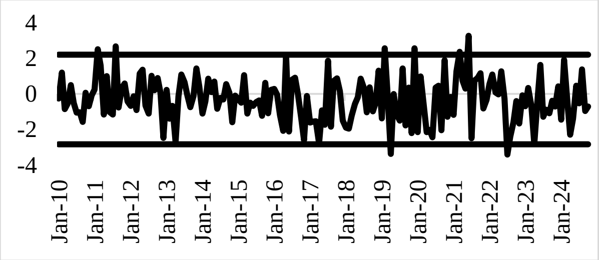


Figure 20: Anomalies in ANSGR by using NCS

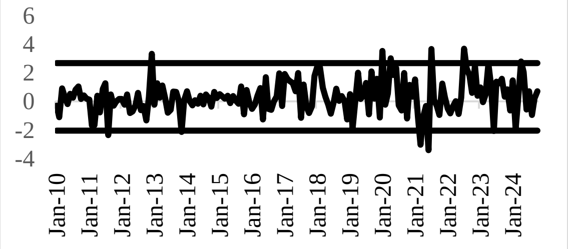


Figure 21: Anomalies in ANSGR by using DUV

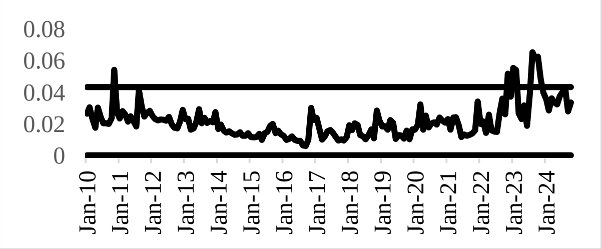


Figure 22: Anomalies in ANSGR by using GK

For RAYSG company, the DUV method estimated nine anomalies, NCS detected 9, Relative Frequency method detected seven and GK approach detected 13 anomalies, as presented in the figures below (Figures 23-26).

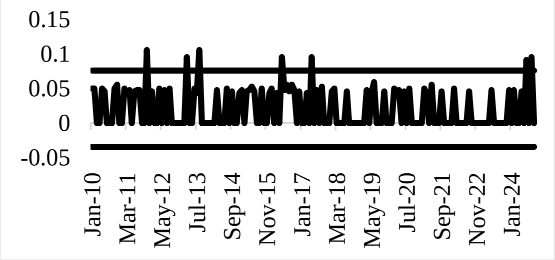


Figure 23: Anomalies in RAYSG by using RF

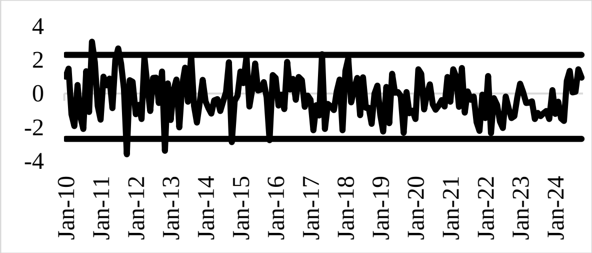
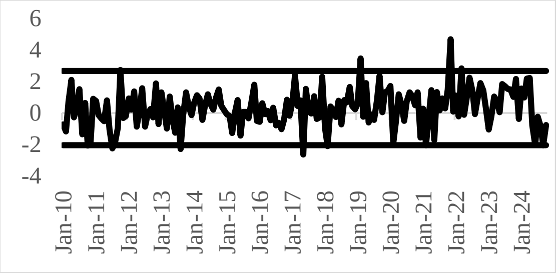


Figure 24: Anomalies in RAYSG by using NCS



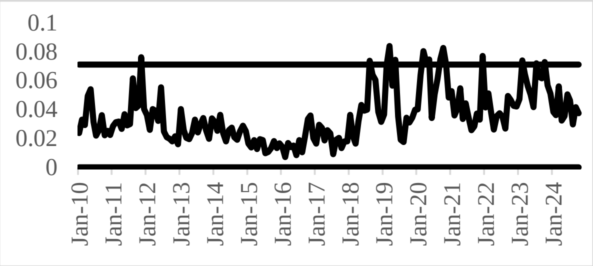
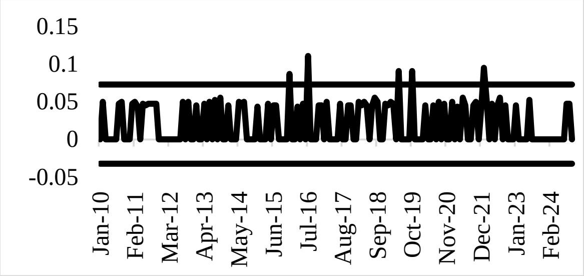


Figure 25: Anomalies in RAYSG by using DUV

Figure 26: Anomalies in RAYSG by using GK

Lastly, for TURSG company, the DUV method estimated seven anomalies, NCS detected seven, RF method detected five and GK approach detected 11 anomalies, as presented in the figures below (Figures 27-30).



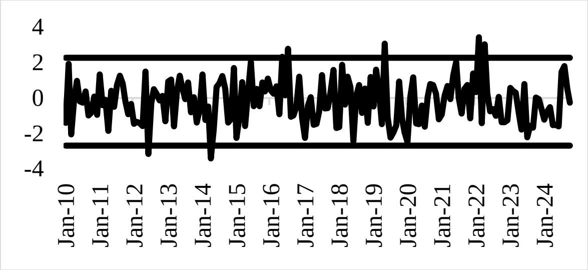
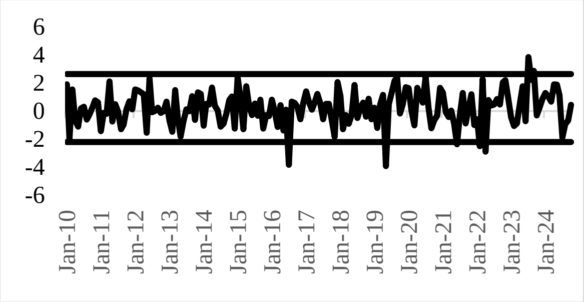


Figure 27: Anomalies in TURSG by using RF

Figure 28: Anomalies in TURSG by using NCS



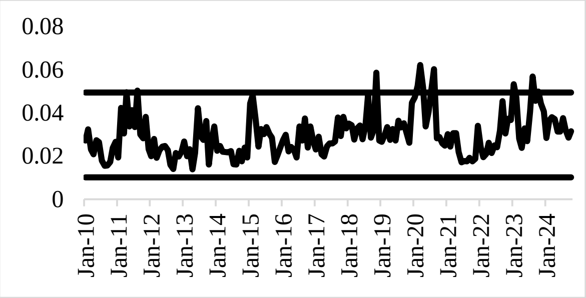


Figure 29: Anomalies in TURSG by using DUV

Figure 30: Anomalies in TURSG by using GK

The analysis revealed 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 Table 2 below, which shows no correlation between GK and RF or GK and NCS, and only a weak correlation between GK and DUV. In contrast, DUV demonstrates a significant but negative correlation with RF and NCS, while NCS and RF exhibit a positive correlation.

Table 2

Correlation Among the Anomaly Detection Methods

Variables	(1)	(2)	(3)	(4)
(1) RF	1.000			
(2) NCS	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 joint anomaly detection from these risk measure, which is presented in the following subsection.

Joint Anomaly Detection Methods

In order to have a joint Anomaly detection, we used two different techniques, Z-Score Normalization and Mahalanobis Distance. After calculating Z-score for each risk measure, we took the average and then calculated the anomalies by using 95% confidence interval ($\cup \pm 2\delta$). The values outside were to be considered as anomalies. For Mahalanobis Distance, we considered four risk measures (DUV, NCS, RF and GK) as vectors and used the distance formula$(\frac{(X-U)}{\delta})^T \varepsilon^{-1} \frac{(X-U)}{\delta}$, which is second moment and then calculated the anomalies by using 95% confidence interval $(\cup \pm 2\delta)$.

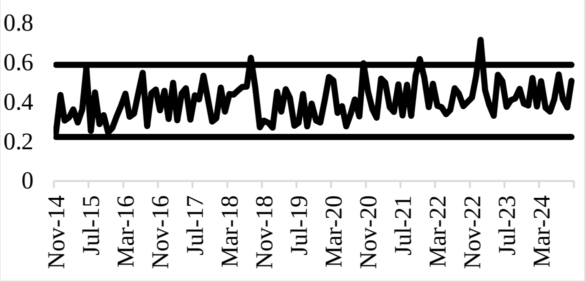


Figure 31: Joint anomaly detection in AGESA by Using Z Score Normalization

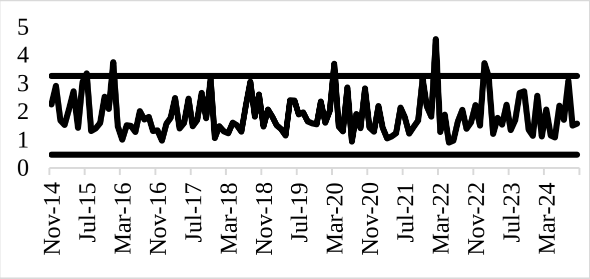


Figure 32: Joint anomaly detection in AGESA by Using Mahalanobis Distance

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. When investigated further, there was only one common anomaly between Z-score and Mahalanobis distance.

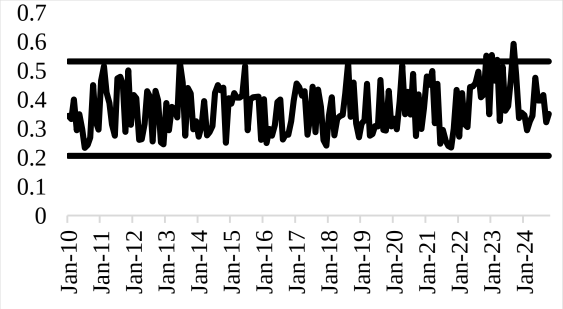


Figure 33: Joint anomaly detection in AKGRT by Using Z Score Normalization

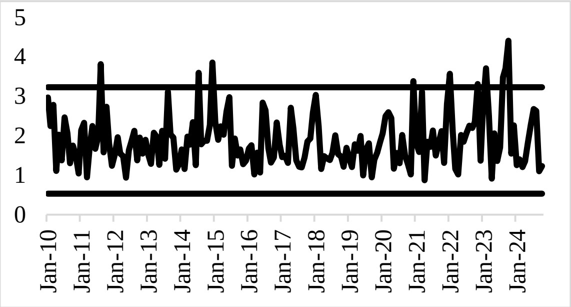


Figure 34: Joint anomaly detection in AKGRT by Using Mahalanobis Distance

Similarly, the number of anomalies in AKGRT insurance company were four when using the Z-Score normalization method and 10 when using Mahalanobis distance. Two anomalies were the same when using different joint anomaly measure. Mahalanobis distance provided better results here as well.

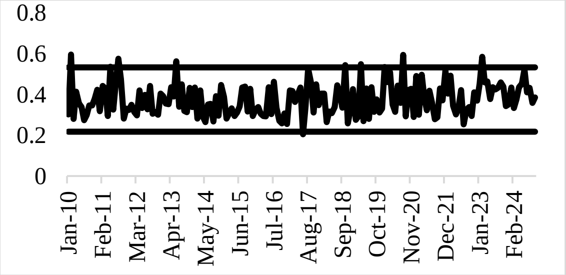


Figure 35: Joint anomaly detection in ANHYT by Using Z Score Normalization

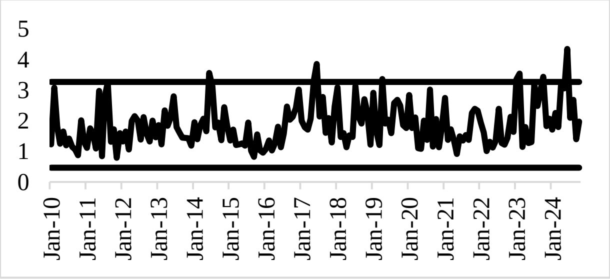


Figure 36: Joint anomaly detection in ANHYT by Using Mahalanobis Distance

In Figure 35 and 36, Mahalanobis distance showed eight anomalies whereas Z-score normalization showed 10, with three anomalies being common between the two. Even number of anomalies were lesser when using Mahalanobis distance but the original data reveals that these 08 are real anomalies as compared to 10 by Z score.

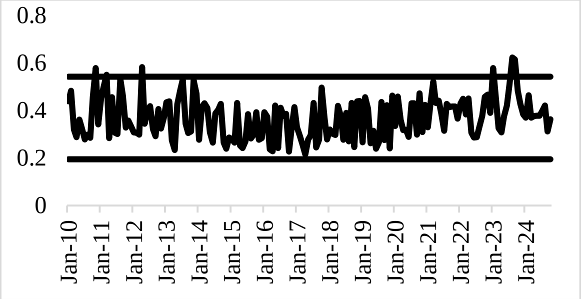


Figure 37: Joint anomaly detection in ANSGR by Using Z Score Normalization

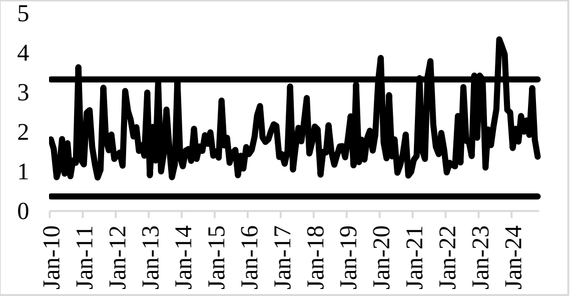


Figure 38: Joint anomaly detection in ANSGR by Using Mahalanobis Distance

In Figures 37 and 38, Z score normalization identified six anomalies in ANSGR insurance company whereas Mahalanobis Distance detect 10. Out of the total, four anomalies are the same (detected by both methods). Again, when we referred to the data, Mahalanobis distance outperformed Z-score normalization.

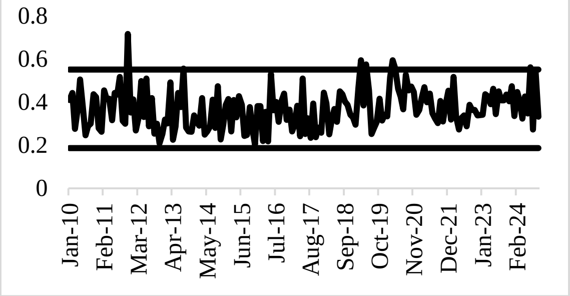


Figure 39: Joint anomaly detection in RAYSG by Using Z Score Normalization

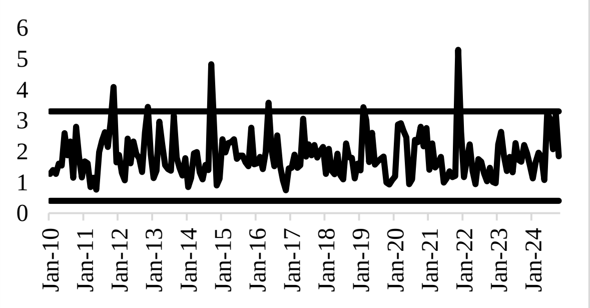


Figure 40: Joint anomaly detection in RAYSG by Using Mahalanobis Distance

For RAYSG, Z Score Normalization detected seven anomalies and Mahalanobis detected six while one anomaly is jointly detected. In term of RAYSG insurance, all 12 anomalies are important but Mahalanobis distance gave the best one.

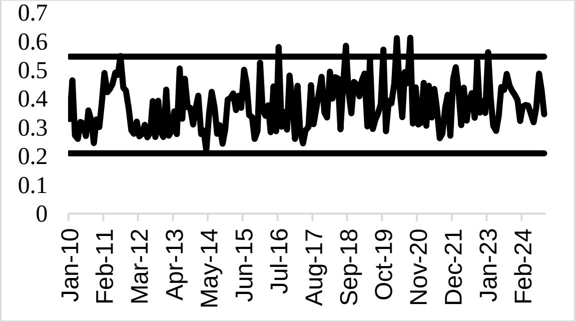


Figure 41: Joint anomaly detection in TURSG by Using Z Score Normalization

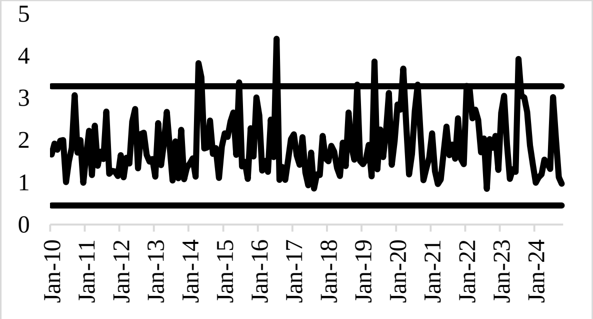


Figure 42: Joint anomaly detection in TURSG by Using Mahalanobis Distance

From figure 41 and 42, total 15 anomalies were detected from the historical data of the TURSG insurance company. 10 anomalies were detected through Mahalanobis Distance, seven through Z-score normalization and two from both the methods.

Therefore, our study advances anomaly detection literature by comparing four risk measures in insurance sector of Türkiye. Unlike traditional approaches, the proposed use of Mahalanobis distance offers greater robustness and efficiency. This method enhances detection accuracy while reducing complexity, providing investors with clearer signals and enabling stock exchange regulators to flag irregularities more effectively, thereby promoting market transparency and fairness.

Conclusion

Our study aimed to detect anomalies in the six insurance companies listed in Borsa-Istanbul using four different measures of risk. These measures of risk demonstrated better performance compared to the traditional model-based anomaly detection methods such as ARCH, GARCH, ARIMA for financial fraud detection in stock exchange historical data. The 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, they mitigated issues related to induced volatility, often introduced by the mean equation of traditional anomaly detection methods. By using these measures of risk, we detected the anomalies and found that our risk measures vary according to the dataset. DUV proved to be more effective for AKGRT, AGESA and ANSGR whereas the GK approach provide better results for ANHYT, RAYSG and TURSG, due to higher daily in their stock prices. The AKGRT dataset, displayed consistently strong detection outcomes across all four risk measures.

We developed a joint anomaly detection method, which is multi-dimensional and robust by using Z-Score Normalization and Mahalanobis Distance approach. Z-Score Normalization treated each measure equally while also ignoring the overlapping effect among the anomaly detection measures. On the other hand, Mahalanobis distance method not only join them but also considered correlations among anomaly detection methods. The results showed that Mahalanobis distance performed well for joint anomaly detection, as it provided more anomalies as compared to Z-Score Normalization and have some same anomalies. However, for RAYSG, the Z-score Normalization performed better as compared to Mahalanobis distance. The existence of the anomalies in the data reflects the presence of the Efficient Market Hypothesis. In essence, the data appears to depart from the predictions of the Efficient Market Hypothesis, implying that market price may not fully reflect all available information.

Based on our conclusions, we suggest that while undergoing 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.

The empirical findings highlight the presence of abnormal return patterns and potential fraud within the insurance sector. Therefore, investors are advised to incorporate risk measure for anomaly detection to enhance portfolio risk management, particularly during periods of high volatility. On the other side, stock exchange regulators should strengthen surveillance mechanisms to identify and mitigate irregular trading behaviors promptly by employing risk measures.

References

Alqurayn, A., Kulendran ,Nada, & and Ihalanayake, R. (2024). An event study of potential insider trading in the Saudi stock market. *Cogent Economics & Finance*, *12*(1), 2367368. https://doi.org/10.1080/23322039.2024.2367368

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. https://doi.org/10.1111/j.1835-2561.2007.tb00443.x

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.

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

Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. *ACM Comput. Surv.*, *41*(3), 15:1-15:58. https://doi.org/10.1145/1541880.1541882

Chang, B. Y., Christoffersen, P., & Jacobs, K. (2013). Market skewness risk and the cross section of stock returns. *Journal of Financial Economics*, *107*(1), 46–68. https://doi.org/10.1016/j.jfineco.2012.07.002

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. https://doi.org/10.1016/S0304-405X(01)00066-6

Comerton-Forde, C., & Putniņš, T. J. (2014). Stock Price Manipulation: Prevalence and Determinants*. *Review of Finance*, *18*(1), 23–66. https://doi.org/10.1093/rof/rfs040

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), 344–401. https://doi.org/10.1016/j.jacceco.2010.09.001

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), Article 1. https://doi.org/10.56301/awl.v5i1.547

Faizan, A., Saeed, M. A., & Kausar, S. (2018). Past and Future of Derivative/Future Market: Substantiation of Calendar Anomalies. *FWU Journal of Social Sciences*, *12*(1), 31–41.

Flores-Guerrero, J. L., Grzegorczyk, M. A., Connelly, M. A., Garcia, E., Navis, G., Dullaart, R. P. F., & Bakker, S. J. L. (2021). Mahalanobis distance, a novel statistical proxy of homeostasis loss is longitudinally associated with risk of type 2 diabetes. *eBioMedicine*, *71*. https://doi.org/10.1016/j.ebiom.2021.103550

Garman, M. B., & Klass, M. J. (1980). On the Estimation of Security Price Volatilities from Historical Data. *The Journal of Business*, *53*(1), 67–78.

Groll, A., Khanna, A., & Zeldin, L. (2024). *A Machine Learning-based Anomaly Detection Framework in Life Insurance Contracts* (No. arXiv:2411.17495). arXiv. https://doi.org/10.48550/arXiv.2411.17495

Hashim, H. A., Salleh, Z., Shuhaimi, I., & Ismail, N. A. N. (2020). The risk of financial fraud: A management perspective. *Journal of Financial Crime*, *27*(4), 1143–1159. https://doi.org/10.1108/JFC-04-2020-0062

Hawkins, D. M. (1980). *Identification of Outliers*. Springer Netherlands. https://doi.org/10.1007/978-94-015-3994-4

Haykir, O., & Yagli, I. (2022a). Speculative bubbles and herding in cryptocurrencies. *Financial Innovation*, *8*(1), 78. https://doi.org/10.1186/s40854-022-00383-0

Haykir, O., & Yagli, I. (2022b). Speculative bubbles and herding in cryptocurrencies. *Financial Innovation*, *8*(1), 78. https://doi.org/10.1186/s40854-022-00383-0

Hodge, V., & Austin, J. (2004). A Survey of Outlier Detection Methodologies. *Artificial Intelligence Review*, *22*(2), 85–126. https://doi.org/10.1023/B:AIRE.0000045502.10941.a9

Jain, A., Nandakumar, K., & Ross, A. (2005). Score normalization in multimodal biometric systems. *Pattern Recognition*, *38*(12), 2270–2285. https://doi.org/10.1016/j.patcog.2005.01.012

Khan, S., Mahmood, F., & Younas, S. (2024). Impact of Fınancıal Knowledge and Investor's Personalıty Traıts on Investment Intentıon: Role of Attıtude and Fınancıal Self Efficacy. *FWU Journal of Social Sciences*, *18*(1). http://121.52.146.40/fwu-journal/index.php/ojss/article/download/3033/23#page=124

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 Trans. Internet Technol.*, *23*(1), 11:1-11:28. https://doi.org/10.1145/3561300

Lee, E. J., Lee ,Yu Kyung, & and Kim, R. (2024). Profitability and herding of trade-based pump-and-dump manipulation. *Applied Economics*, *56*(20), 2375–2385. https://doi.org/10.1080/00036846.2023.2182405

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. https://doi.org/10.1108/AJAR-09-2018-0032

Palacio, S. M. (2019). Abnormal Pattern Prediction: Detecting Fraudulent Insurance Property Claims with Semi-Supervised Machine-Learning. *Data Science Journal*, *18*, 35–35. https://doi.org/10.5334/dsj-2019-035

Pareek, K., Sharma, R., Sharma, S., & Rao, A. (2022). Machine Learning In Fraud Detection and Prevention. *Tuijin Jishu/Journal of Propulsion Technology*, *43*(4), Article 4. https://doi.org/10.52783/tjjpt.v43.i3.2344

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. https://doi.org/10.1111/0022-1082.275500

Salas-Molina, F., Rodríguez-Aguilar, J. A., Serrà, J., Guillen, M., & Martin, F. J. (2017). *Empirical analysis of daily cash flow time series and its implications for forecasting* (No. arXiv:1611.04941). arXiv. https://doi.org/10.48550/arXiv.1611.04941

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*, Article 41. https://doi.org/10.31590/ejosat.1063728

Seyhun, H. N. (1986). Insiders' profits, costs of trading, and market efficiency. *Journal of Financial Economics*, *16*(2), 189–212. https://doi.org/10.1016/0304-405X(86)90060-7

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.

Teker, D. L., Teker, S., & Gümüştepe, E. D. (2024). BACKCASTING BITCOIN VOLATILITY: ARCH AND GARCH APPROACHES. *PressAcademia Procedia*, *20*(1), Article 1. https://doi.org/10.17261/Pressacademia.2024.1918

Wells, J. T. (2017). *Corporate Fraud Handbook: Prevention and Detection*. John Wiley & Sons.

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. https://doi.org/10.1016/j.jimonfin.2022.102683

Zhang, M., Li, T., Yu, Y., Li, Y., Hui, P., & Zheng, Y. (2022). Urban Anomaly Analytics: Description, Detection, and Prediction. *IEEE Transactions on Big Data*, *8*(3), 809–826. IEEE Transactions on Big Data. https://doi.org/10.1109/TBDATA.2020.2991008