Journal of Economic Cooperation and Development, **46**, 4 (2025), 85-112

Evaluating Machine Learning and Deep Learning Algorithms for Financial Anomaly Detection: A Comparative Study

Ahmet Akusta[1], Mehmet Nuri Salur[2] and Ahmet Şahbaz[3]

ABSTRACT

This paper aims to provide a comprehensive comparative analysis of various algorithms for anomaly detection in financial time series data, specifically focusing on Ford Otosan stock, the BIST100 index, and the USD/TRY exchange rate. The study evaluates the performance of algorithms, including Isolation Forest, Single-Class Support Vector Machines, Local Outlier Factor, DBSCAN, KMeans, and Autoencoders, utilizing metrics such as accuracy, precision, recall, and F1 score. These insights contribute to the existing body of knowledge by offering a detailed comparison of machine learning and deep learning techniques, providing valuable implications for risk management and investment strategies. The paper acknowledges the study's limitations, including the relatively short analysis period and the specific set of algorithms used. The findings reveal that KMeans is the most effective model for anomaly detection, demonstrating high accuracy and sensitivity. Isolation Forest and Autoencoders also perform well but have certain limitations.

ملخص

تهدف هذه الدراسة إلى تقديم تحليل مقارن شامل لعدة خوارزميات في كشف الشذوذ ضمن بيانات السلاسل الزمنية المالية، مع التركيز على سهم فورد أوتوسان، ومؤشر BIST100، وسعر صرف الدولار/الليرة التركية. تم تقييم أداء الخوارزميات، بما في ذلك "غابة العزل"، وآلات المتجه الداعم أحادية التصنيف، وعامل الشذوذ المحلي، وخوارزميةDBSCAN ، وخوارزميةKMeans ، والمشفّرات التلقائية، باستخدام معايير الدقة، ومعامل الاسترجاع، والتذكّر، ومعامل F1. تساهم نتائج الدراسة في إثراء المعرفة الحالية من خلال المقارنة التفصيلية بين تقنيات التعلم الآلي والتعلم العميق،

[1]Rectorate, Konya Technical University, Konya, Türkiye..
E-mail: ahmetakusta@hotmail.com
[2] Faculty of Political Science, Necmettin Erbakan University, Konya, Türkiye.
E-mail: nsalur@erbakan.edu.tr
[3] Faculty of Political Science, Necmettin Erbakan University, Konya, Türkiye.
E-mail: asahbaz@erbakan.edu.tr

وتوفر دلالات تطبيقية في مجال إدارة المخاطر واستراتيجيات الاستثمار. وتقر الدراسة بوجود بعض القيود، أبرزها قصر فترة التحليل ومحدودية عدد الخوارزميات المستخدمة. تشير النتائج إلى أن خوارزمية KMeans هي الأكثر فعالية في كشف الشذوذ، حيث أظهرت مستويات عالية من الدقة والحساسية. كما أظهرت كل من غابة العزل والمشفّرات التلقائية أداء جيدا، مع بعض القيود المحددة.

RÉSUMÉ

Cet article vise à fournir une analyse comparative complète de divers algorithmes de détection d'anomalies dans les séries chronologiques financières, en mettant particulièrement l'accent sur l'action Ford Otosan, l'indice BIST100 et le taux de change USD/TRY. L'étude évalue les performances d'algorithmes tels que : Isolation Forest, Single-Class Support Vector Machines, Local Outlier Factor, DBSCAN, KMeans et Autoencoders, à l'aide de mesures telles que la précision, la spécificité, la sensibilité et le score F1. Ces résultats contribuent aux connaissances actuelles en fournissant une comparaison détaillée entre les techniques d'apprentissage automatique et d'apprentissage profond, apportant ainsi des informations utiles pour la gestion des risques et les stratégies d'investissement. L'article reconnaît les limites de l'étude, notamment la période d'analyse relativement courte et l'ensemble limité d'algorithmes utilisés. Les résultats révèlent que KMeans est le modèle le plus efficace pour détecter les anomalies, car il fait preuve d'une grande précision et d'une grande sensibilité. Isolation Forest et Autoencoders fonctionnent également bien, mais présentent certaines limites.

Keywords: Anomaly detection, Machine learning, Deep learning, BIST100 index

JEL Classification: C45, G15, G17

1. Introduction

The utility of anomaly detection goes beyond financial applications. It plays a critical role in identifying unusual behavior in various industries, such as fraud detection in finance and insurance, anomaly pattern identification in medical diagnostics, and fault detection in safety-critical systems (Ray et al., 2018). Especially in the financial sector, effective anomaly detection can significantly reduce losses due to credit card fraud, thus protecting financial assets by enhancing customer confidence (Lok et al., 2022). Although anomaly detection varies across domains and systems, it is often formally defined as "the problem of

finding patterns in data that do not conform to expected behavior" (Guggilam et al., 2019). With a broad definition, anomaly detection defines the primary objective as identifying observations that are significantly rare or deviate from the majority (Y. Li et al., 2019).
The evolution of edge computing has significantly impacted anomaly detection methods by providing more sensitive detection mechanisms (Yu et al., 2021). The diversity of anomaly detection methodologies encompasses some essential techniques, including classification-based, nearest neighbor, clustering, statistical, information theory-based, and spectral theory approaches (Wang et al., 2013).

Anomaly detection is used in many industries. Particularly in healthcare, critical infrastructures, and security applications where rapid detection of anomalies is critical, timely and effective anomaly detection mechanisms are essential (Schneider and Xhafa, 2022).

Anomaly detection in intrusion detection systems focuses on modeling the expected behavior of system users and detecting deviations from this norm. In cybersecurity, these deviations are considered indicators of potential leaks or threats (Mazarbhuiya and Sahmoudi, 2023). The comprehensive approach to anomaly detection across various domains contributes significantly to the advancement of detection techniques. In this way, the security and efficiency of various systems and applications are ensured (Dhadhania, 2023).

Anomaly detection in finance can significantly improve operational efficiency in business processes (Cruz et al., 2023). Integrating machine learning (ML) and deep learning (DL) algorithms into financial anomaly detection increases the sensitivity and efficiency in detecting financial irregularities.

We position this research at the intersection of machine learning (ML) and deep learning (DL) applications in financial anomaly detection. We aimed to understand various algorithms for detecting irregularities in financial datasets. In this study, we compared the performance of several algorithms along the dimensions of accuracy, precision, recall, and F1 score. The algorithms used include Isolation Forest, One-Class Support Vector Machines, Local Outlier Factor, DBSCAN, K-Means, and Autoencoders. The study analyzed various financial datasets, including stock prices, indices, and exchange rates.

In the following sections, we first analyze financial time series data, mainly focusing on Ford Otosan's stock price, BIST100 index, and USDTRY exchange rate from October 2022 to January 2024. The initial analysis involves summarizing the data with descriptive statistics to understand key characteristics and trends. We also visualize the time series to detect significant anomalies and correlations between variables. We use Machine Learning and Deep Learning models to detect anomalies and compare algorithms using performance metrics. We investigate the relationship between market anomaly, exchange rate anomaly, and Ford Otosan's stock price anomaly.

2. Literature Review

Ahmed et al., (2016) performed a deeper study of anomaly detection techniques based on clustering in finance, focusing on renewed interest in identifying fraud and challenges that arose from the data of practical use. This paper remains outstanding in two aspects: giving comparative analysis with a discussion on synthetic data usage for validation of approaches to anomaly detection and giving forecasting potential for use in financial markets.

Ahmed et al., (2017) discussed standard anomaly detection techniques in big data applied to the financial market, particularly historical Australian Security Exchange (ASX) trading data. They studied the performance of the detection techniques using LOF and CMGOS. They set up these methods to be effective for the detection of rare anomalies in voluminous financial data.

In the model proposed by D. Xu et al., (2018) for improved data anomaly detection, the authors named it SA-iForest. Their approach selects isolation trees based on precision and diversity with optimum optimization in constructing the forest. This is important as it improves the detection accuracy and execution efficiency compared to traditional methods.

Kulkarni et al., (2017) researched network-based anomaly detection to find potential illegal insider trading activities, mainly from data from the United States Securities and Exchange Commission. They modeled networks depicting relations among insider traders to capture patterns

related to potential anomalies. The idea, underlines the importance of an empirical approach in dealing with insider trading cases.

The work presented by D. Huang et al., (2018) developed a new framework of CoDetect, which jointly utilizes information from networks and features in detecting financial fraud effectively. Their model overcomes some of the limitations of conventional methods and can concurrently establish fraud activities with their associated feature patterns. This proves to be an efficient approach to fighting the extremes of financial fraud, especially money laundering.

C. Zhang et al., (2019) based on the MSCRED framework to propose an unsupervised anomaly detection and diagnosis network for multivariate time series data. These are structured multiscale signature matrices representing the system status of different time steps. An added novel part is a convolutional encoder and attention-based ConvLSTM network that enabled the inter-sensor features to capture the originating relationship of sensors in chronological order. Their method outperforms the more elementary benchmark methods in both the synthetic and natural datasets of power plant data, exhibiting high performance in anomaly detection and diagnosis with robustness against noise and anomalies of varying severity.

Lokanan et al., (2019) tested credit quality of firms by applying a dynamic approach for anomaly detection based on the Mahalanobis distance. The model proposed approach taken in the financial statements of Vietnamese listed firms between 2001 and 2016 enabled the ranking of the reports in terms of creditworthiness. The model proposed for anomaly detection enables limitation over a simple assumption concerning the statistical distribution of the data and data availability.

M. Huang et al., (2019) presented a hybrid algorithm for forecasting financial time series data by fusing OVDBCSAN with SVR for financial clustering to enhance forecasting accuracy. Also, they proved the potential of their method in the analysis of financial time series data for predicting financial or stock prices.

Ghrib et al., (2020) proposed a hybrid methodology for detecting anomalies in high-dimensional time series data. The proposed method combined the LSTM Autoencoder and the SVM classifier. According to

the statistics, this approach efficiently encodes the time series data and significantly reduces the correlation between normal and abnormal records. Their approach outperforms the state-of-the-art in terms of anomaly detection.

Braei and Wagner, (2020) conducted a survey on state-of-the-art anomaly detection in univariate time series through statistical, machine learning, and deep learning techniques. The work then assesses computational efficiency and compares performance results with publicly presented datasets.

Literature from 2020 to 2021 represents an alliance of the most innovative approaches toward anomaly and jump detection in financial time series by advanced machine learning, deep learning, and data mining techniques. In a big way, it contributes significantly to finance and data sciences by revealing new ways of analyzing financial markets' behavior, discovering their irregularities, and forecasting market volatility.

Au Yeung et al., (2020) developed a hybrid machine-learning model that combines an LSTM neural network for prediction of jumps in financial time series with the general machine learning pattern recognition model to detect jumps; it does not require a predefined parameter for the jump detection, such as the threshold value acting as a jump parameter with the other methods. The newly developed model has undergone empirical testing across the stock markets worldwide and has developed a higher testing accuracy than traditional methodologies in jump detection.

Toshniwal et al., (2020) discussed the various techniques applied to implement anomaly detection with machine learning. They strongly advocated correctly detecting rare events or anomalies in datasets. Their survey reveals the significance of selecting the correct anomaly detection algorithms that depend on input data, anomaly type, and domain knowledge.

Yang et al., (2020) focused on the forecast of market volatility, using big data analytics and support vector machines. On the other hand, they based it on high-frequency financial data to serve a similar purpose. High ranking is vital in confirming the importance of volatility as a

market indicator for risks, along with forecasting superiority over HAR-lnRV models.
Albu and Lupu, (2020) used a very modern kind of the neural network, special Autoencoder LSTM, to analyze anomalies in stock market indices. The present study has shown economically significant patterns and anomalies related to major events, like the current pandemic crisis. This demonstrates that neural networks can enhance systemic risk detection and early warning systems.

G. Li and Jung, (2021) proposed an approach of detecting financial time series abnormality by turning them into dynamic graphs. They have proposed a model called dynamic graph embedding of the financial indices for mapping spurious relationships into an embedding space. The effectiveness of this method in detecting abnormalities was higher.

In a related work, (Choi et al., 2021) reviewed state-of-the-art deep learning approaches that deal with anomaly detection in time-series data. The works have shown promising performance over several benchmark datasets and significant improvements in dealing with long-range sequences. The other relationship is in its claim about the need for effective deployment of models, which quoted necessary domain knowledge.

J. Li et al., (2021) proposed a clustering-based approach for multivariate time series anomaly detection. They applied the sliding window technique and extended fuzzy clustering of their design. With the enhancement of particle swarm optimization, the method was tested on synthetic sets of data and some real-world datasets. This routine shows promise for health care, finance, and many other essential fields where anomaly detection is crucial.

Da Silva Arantes et al., 2021 presented an unsupervised technique to detect anomalies in industrial machines. They used predictive maintenance based on statistical features of the sensor data. Their method achieved high AUC values over various datasets to reduce financial costs due to machine failure and production downtime.

Zhou et al., (2021) presented an anomaly detection process of time series based on a combination model. Their process represents data, taking both original data and amplitude change data into account, and

captures shape and morphological features. It outperforms state-of-the-art methods as built-in.
Lesouple et al., (2021) suggested the Generalized Isolation Forest (GIF) algorithm. Extended Isolation Forest increased the shortcomings of tree construction in the GIF and reduced the execution time. It performs more or less the same task that the EIF does but in a more proper way.

Al Farizi et al., (2021) conducted a systematic literature review on improvements to the Isolation Forest (IF) algorithm for anomaly detection. Their review categorizes the solutions to IF's weaknesses into pre-IF, post-IF, and method improvements. It highlights the ongoing research efforts to enhance IF's capability to deal with high-dimensional data and its application across various fields.

Sridhar and Sanagavarapu (2021) detected market manipulation through an Extreme Learning Machine framework, ELMAD, of stock market price and volume data from the Bombay Stock Exchange. Price and volume manipulation with the ELM-AD model achieved high detection rates. This approach underscores the capability of rapid and high-quality machine learning techniques to identify market abuse.

Shah et al., (2021) applied and evaluated a model to forecast anomalies of the time series data within the SENSEX and NIFTY50 with implementations of Long Short-Term Memory (LSTM) neural networks. It is built from an LSTM autoencoder; deep learning models detect major market events, such as sudden spikes and declines or changing trends and level shifts in stock prices.

Crépey et al., (2022) combined the neural network with PCA in a novel way to improve the anomaly detection ability of financial time series. Their PCA NN method extracts important features and identifies contaminated time series to define an anomaly score by feedforward neural networks efficiently.

Huet et al., (2022) criticized classical precision/recall metrics in this context and provided a robust extension in a parameter-free way by the "affiliation" between ground truth and prediction sets. Considering duration measures between actual events and predictions in such metrics offers a much more describable evaluation of the anomaly detection algorithms.

The literature from 2022 to 2023 expands the exploration of anomaly detection in financial markets. It focuses on insider trading, multivariate time series analysis, and applying novel algorithms to tackle the challenges of identifying anomalies in stock market data.

Shein et al., (2022) studied the application of an analysis of sequential fences to detect insider trading behavior on China's stock market. They find that sequential fences can detect unusual market activity. This paper emphasizes the potential for statistical methodologies to reveal the presence of insider trading practices.

G. Li and Jung, (2023) assessed deep learning for anomaly prediction in multivariate time series in their work. They defined anomalies as abnormal time points, intervals, and series. However, their study distinguished the associated challenges from the intelligibility of these anomalies.

H. Xu et al., (2023) addressed the limitations of the iForest algorithm. They have proposed a Deep Isolation Forest model that uses neural networks for data mapping and ensembles of random representation. The technique contains essential improvements related to the detection of anomalies among datasets.

Bachelard et al., (2023) proposed a randomized geometric tools for detecting low-volatility anomalies in stock markets. The method samples and estimates volumes of complex spherical patches, which brings new light on portfolio performance characteristics and challenges classical methods in detecting financial anomalies.

3. Methodology

This chapter provides a methodological framework for analyzing machine learning and deep learning algorithms, emphasizing the best ways to compare the effectiveness of such using abnormal detection financial time series data. To this purpose, it emphasizes isolation forests, one-class SVM, local outlier factors, DBSCAN, K-means, and autoencoder algorithms. The chapter will investigate the effective way of utilizing algorithms, besides making a detection, ensuring that the

anomalous patterns are evidenced in various financial datasets, with a particular emphasis on Ford Otosan Stock, BIST100, and USDTRY.

3.1. Data Definition

The dataset includes daily values of Ford Otosan Stock, BIST100, and USDTRY (US Dollar/Turkish Lira exchange rate). The data is collected from the Yahoo Finance Database. It covers 15 months from October 2022 to January 2024. This data provides an overview of market dynamics.

Figure 1. Historical plots of the variables

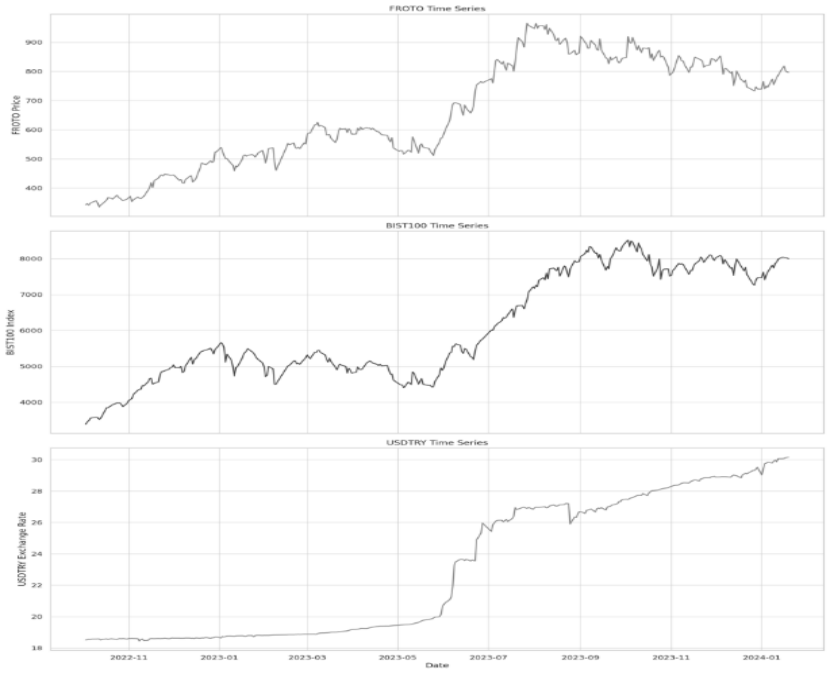


Figure 1 presents time series plots for FROTO stock prices, the BIST100 index, and the USD/TRY exchange rate. These plots show that FROTO stock and the BIST100 index follow similar trends. However, FROTO exhibits more volatility and sometimes moves independently. The sudden increases in the USD/TRY exchange rate do not affect FROTO stock prices, indicating that FROTO occasionally behaves independently of USD/TRY movements.

Table 1. Descriptive Statistics

	FROTO	BIST100	USDTRY
Count	**328**	**328**	**328**
Mean	**658.235367**	**6083.285662**	**23.074028**
Std	**184.05607**	**1489.747342**	**4.423615**
Min	**335**	**3392.100098**	**18.444**
25%	**512.774994**	**4948.675049**	**18.794761**
50%	**613.25**	**5431.800049**	**20.058141**
75%	**834.324982**	**7717.475098**	**27.238735**
Max	**965**	**8513.5**	**30.153601**

The statistics in Table 1 show the main characteristics of FROTO, BIST100, and USDTRY variables. The high standard deviations of FROTO and BIST100 indicate that these variables show significant changes over time. USDTRY's lower standard deviation indicates a more stable change.

Table 2. Correlation Matrix

	FROTO	BIST100	USDTRY
FROTO	**1**	**0.913179**	**0.897671**
BIST100	**0.913179**	**1**	**0.929117**
USDTRY	**0.897671**	**0.929117**	**1**

The correlation matrix in Table 2 shows strong positive relationships between variables. There is a 91.3% correlation between FROTO and BIST100, 89.8% correlation between FROTO and USDTRY, and 92.9% correlation between BIST100 and USDTRY. These high correlation values indicate that the variables tend to move together.

Table 3. Regression Model Results

Model No	Dependent Variable	Independent Variable	$R2$	β	p
Model 1	**FROTO**	**BIST100**	**0.839**	**0.7623**	**0.000**
Model 2	**FROTO**	**USDTRY**	**0.809**	**0.6937**	**0.000**
Model 3	**BIST100**	**USDTRY**	**0.838**	**0.7007**	**0.000**

Model 1 shows a strong positive relationship between the BIST100 index and FROTO share prices. The p-value of the independent variable is 0.000, which indicates that the model is statistically significant.

Model 2 shows a strong positive relationship between the USDTRY exchange rate and FROTO share prices. The p-value of the independent variable is 0.000, which indicates that the model is statistically significant.

Model 3 shows a strong positive relationship between the USDTRY exchange rate and the BIST100 index. The p-value of the independent variable is 0.000, which indicates that the model is statistically significant.

3.2. Anomaly Detection

Anomaly detection is the task of finding patterns or values that are significantly different from the majority of the data. Anomaly detection is vital in various domains (Siegel, 2020). Traditional methods rely on measures of distance and density-based approaches, mathematical techniques, or clustering-based techniques such as isolation forest and cluster-based local outlier or any other supervised-based learning algorithm that may result in disparities when dealing with large datasets and complex data (Siegel, 2020). The superiority of deep learning approaches such as Generative Adversarial Networks (GAN), 1-D Convolutional Neural Networks (1DCNN), or multivariate datasets is profound, and this kind of application assists in identifying subtle anomalies in different data types (Siegel, 2020).

The performance differences between traditional and deep learning-based methods have been highlighted, with deep learning often superior to traditional methods in terms of accuracy and scalability, especially for fluid data or unstructured data types (Siegel, 2020). However, the choice of predication model algorithm depends on some factors or requirements of the application because while the deep learning model is highly flexible and scalable, traditional methods are generally more interpretable and robust. Traditional methods often need help dealing with large or noisy datasets, which can lead to high false favorable rates (Foorthuis, 2020). Meanwhile, autoencoders and convolutional neural networks are deep learning approaches that have proven very good at

capturing complex patterns and, in many cases, being better than the accuracy of their traditional counterparts. These advanced techniques leverage large-scale datasets and intensive computational power to model complex relationships in data (X. Xu et al., 2023; J. Zhang et al., 2021).

Deep learning-based anomaly detection often revolves around generative models because they are inherently unsupervised but face challenges in training (Monakhov et al., 2023). The scarcity of deep-learning approaches for anomaly detection suggests that more research is needed in this area (Chalapathy, 2019).

Table 3. Algorithms used and characteristics

Algorithm	Architecture	Characteristics	Reference
Isolation Forest	**Decision trees**	**It detects anomalies by isolating observations using randomly selected features and splitting values.**	**www.scikit-learn.org**
Single Class SVM	**Kernel-based classification algorithm**	**It assumes all data belong to the same class and learns a boundary to separate them from possible anomalies.**	**www.scikit-learn.org**
Local Outlier Factor	**Distance-based algorithm**	**It calculates a local outlier factor score based on the density of observations and the density of their neighbors.**	**www.scikit-learn.org**
DBSCAN	**Density-based clustering algorithm**	**It defines clusters based on core instances (having a certain number of neighbors) and non-core instances (neighbors of core instances).**	**www.scikit-learn.org**
K-Means	**Centroid-based clustering algorithm**	**It divides the data into clusters with equal variance, minimizing the within-cluster total squares.**	**www.scikit-learn.org**
Autoencoders	**Neural networks that encode and decode data**	**It is used for data denoising and dimensionality reduction and learning latent data representations.**	**www.keras.io**

Autoencoder is an unsupervised learning algorithm that learns data representations for dimensionality reduction or anomaly detection by training the model to reconstruct the input data. It focuses on capturing the most essential features of the input data (Ferreira and Cortez, 2023). KMeans is a clustering algorithm that partitions data into K clusters based on the mean distance between data points and cluster centroids. Although it is not explicitly designed for anomaly detection, it can be used for clustering normal data points (Mensi et al., 2021).

The Local Outlier Factor (LOF) is generally referred to as a density-based algorithm for identifying outliers, which are based on the local deviation of the density regarding a data point concerning its neighbors. It effectively identifies local outliers in dense clustering (Shriram & Sivasankar, 2019).

One-class SVM is a support vector machine algorithm that learns normal data boundaries and identifies anomalies with data points outside such boundaries. It can very well capture the shape of the normal data distribution (Shriram & Sivasankar, 2019).

DBSCAN is a density-based clustering algorithm that detects data points in low-density regions and groups closely seated data points while detecting outliers. It can work effectively with sets of different shapes and sizes (Degirmenci & Karal, 2022).

Autoencoders can extract very complex patterns of data and accurately reconstruct normal data samples only from the encoded and decoded input in several layers of neural networks. Problems occur when it comes to high-dimensional data, where the increased dimensionality would increase complexity, and with increased feature volume, it can quickly saturate the network, resulting in problems during the reconstruction (Ferreira & Cortez, 2023). Similarly, KMeans is not explicitly designed to detect anomalies. Nevertheless, it can identify outliers as data points far from cluster centroids (Mensi et al., 2021). Local Outlier Factor (LOF) effectively identifies local outliers within dense clusters. However, it may struggle with varying density and high-dimensional data (Shriram & Sivasankar, 2019).

Furthermore, OneClass SVM captures the shape of the normal data distribution effectively. It identifies anomalies outside the learned boundaries (Shriram & Sivasankar, 2019). Isolation Forest is effective in isolating anomalies and is suitable for high-dimensional data. However, it may struggle with global outliers (Ferreira & Cortez, 2023; Mensi et al., 2021). DBSCAN is effective in identifying outliers in low-density regions. It handles clusters of varying shapes and sizes (Degirmenci & Karal, 2022).

Advantages include Autoencoder's ability to capture complex patterns and provide a data-driven approach to anomaly detection (Ferreira & Cortez, 2023). Similarly, KMeans is simple and computationally efficient for identifying global outliers (Mensi et al., 2021). Local Outlier Factor (LOF) effectively identifies local outliers within dense clusters (Shriram & Sivasankar, 2019). Furthermore, OneClass SVM captures the shape of the normal data distribution and is effective for high-dimensional data (Shriram & Sivasankar, 2019). Additionally, Isolation Forest is suitable for high-dimensional data and does not rely on distance or density measures (Ferreira & Cortez, 2023; Mensi et al., 2021). Lastly, DBSCAN effectively handles clusters of varying shapes and sizes and identifies outliers in low-density regions (Degirmenci & Karal, 2022).

Disadvantages include Autoencoder's struggle with high-dimensional data and the need to tune hyperparameters (Ferreira & Cortez, 2023) carefully. Similarly, KMeans may need help with non-linear data and varying cluster densities (Mensi et al., 2021). Local Outlier Factor (LOF) may need help with varying density and high-dimensional data (Shriram & Sivasankar, 2019). Furthermore, OneClass SVM is sensitive to the choice of kernel and parameters and may struggle with complex data distributions (Shriram & Sivasankar, 2019). Additionally, Isolation Forests may need help with global outliers and require careful tuning of hyperparameters (Ferreira & Cortez, 2023; Mensi et al., 2021). Lastly, DBSCAN is sensitive to the choice of distance metric and the need to specify the minimum number of points in a neighborhood (Degirmenci & Karal, 2022).

4. Comparative Analysis

4.1. Performance Evaluation Metrics

The accuracy, precision, recall, F1 score metrics are extensively used to test and compare algorithms. Therefore, one should be able to contrast the performance of the algorithms with these quantified metrics to have a clear conception of the practical application of anomaly detection within financial datasets. The accuracy, precision, recall, and F1 score metrics used in this study are formulated as follows (Elmrabit et al., 2019):

$$Accuracy = \frac{Number\ of\ Correct\ Predictions}{Total\ Number\ of\ Predictions} \quad (1)$$

$$Precision\ = \frac{Number\ of\ True\ Positives\ (TP)}{True\ Positives\ (TP) + False\ Positives\ (FP))} \quad (2)$$

$$Recall = \frac{Number\ of\ True\ Positives\ (TP)}{True\ Positives\ (TP) + False\ Negatives\ (FN)} \quad (3)$$

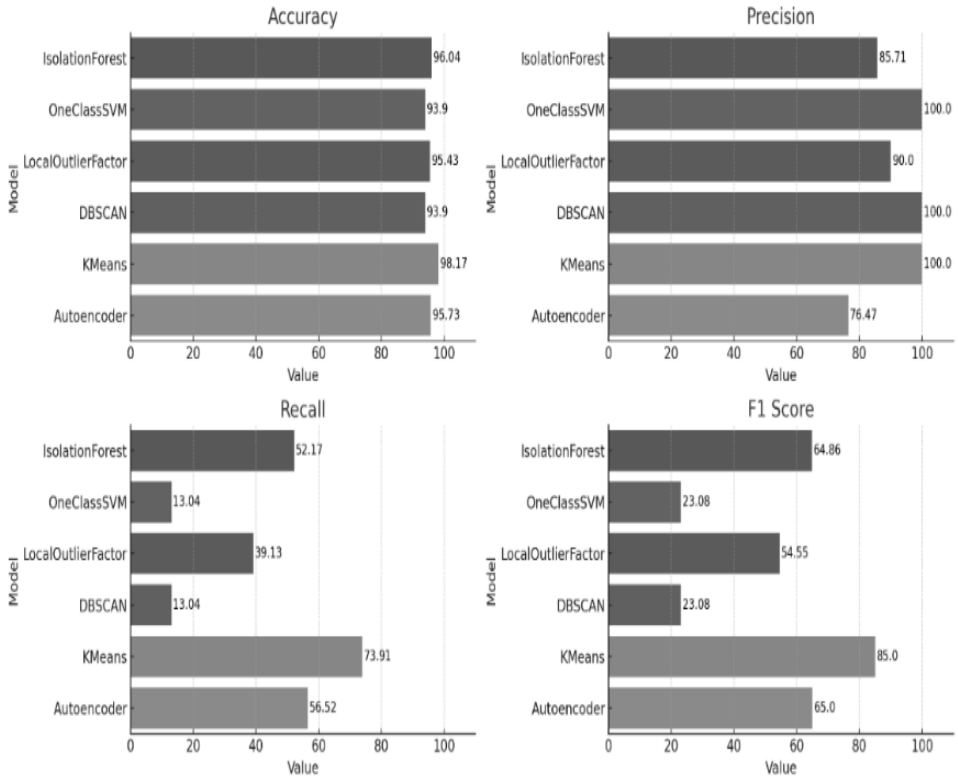
$$F1\ Score = 2x\frac{Precision \times Recall}{Precision + Recall} \quad (4)$$

Accuracy is the ratio of correctly predicted observations to total observations. We use this metric to measure how often the model is correct. Precision measures how many of the identified positive cases were actually positive. It is calculated as the number of true positives divided by the sum of true positives and false positives. Recall shows how many true positives were correctly detected. The F1 Score is the harmonic average of Precision and Recall.

The comparative performance of each algorithm in the context of anomaly detection in financial time series data will be assessed using these metrics. It will shed light on the effectiveness of the algorithms in practical applications.

4.2. Comparison of Models

Figure 2. Comparison of Model Metrics



The Isolation Forest model has a very high overall accuracy at 96.04%. It is also highly precise at 85.71% in detecting any anomaly, meaning most of them are actually true anomalies. However, it has moderate sensitivity, 52.17%, missing many of these anomalies. Therefore, the isolation forest is a dependable technique for detecting anomalies, but it may overlook certain anomalies.

OneClass SVM model has a perfect precision of 100%, meaning everything the model is positive about must be an anomaly. However, sensitivity is fragile, at 13.04%, implying that this model does not detect most anomalies in the data. Although this model accurately detects positive cases, it discovers a few anomalies.

The LOF model's accuracy score was 95.43%, and the precision was 90%. However, sensitivity is low, at 39.13%. Results indicate that most anomalies correctly detected by the model are indeed anomalies, but they miss many. The LOF model is reliable but fails to detect many anomalies.

The DBSCAN model has a precision of 100%, just like the One-Class SVM, but its sensitivity is low, at 13.04%. It gets positive predictions but misses many anomalies because of this necessarily low sensitivity.
The KMeans model has the highest success rate, 98.17%, and the highest precision and recall. First, this means that all positive marks are indeed anomalies. Besides, it has a high sensitivity of 73.91%, so most of the true anomalies will be captured. This model would assure reliable and efficient anomaly detection.

The Autoencoder model proposed attains perfect accuracy, with 95.73% balanced performance. It showed a sensitivity of 76.47% and a precision of 56.52%, meaning it could detect many anomalies without a performance as high as one of the KMeans and Isolation Forest methods.

The KMeans model shows the highest performance for anomaly detection. With high accuracy and high precision, all the anomalies it detects are correct. The Isolation Forest model performs well with high accuracy and precision but may miss some anomalies. The Autoencoder model has a balanced performance but does not have as high metrics as KMeans. The Local Outlier Factor (LOF) model is reliable but can miss many anomalies. Despite their high precision, OneClass SVM and DBSCAN models miss many anomalies due to low sensitivity.

According to these evaluations, KMeans is the most suitable model for anomaly detection in the BIST100 market. This model can detect anomalies both accurately and effectively.

Figure 3. Anomalies detected by the models (FROTO-BIST100-USDTRY)

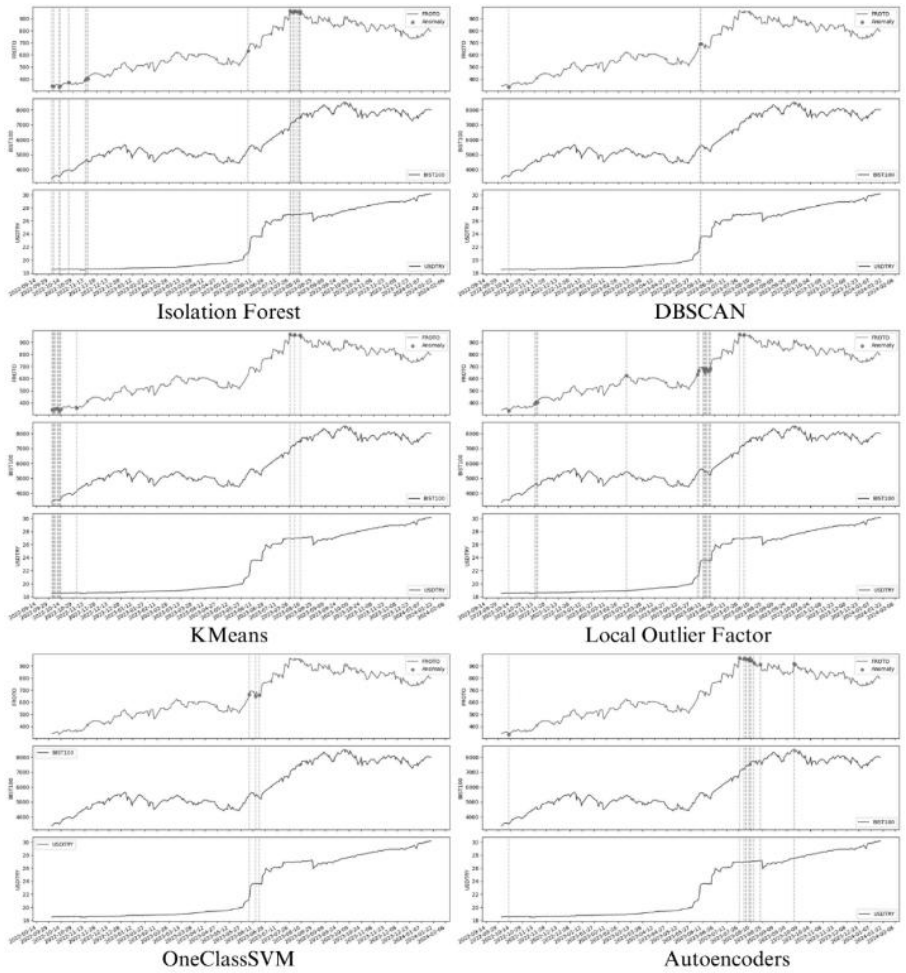


Figure 3 shows the anomalies detected in the Ford Otosan stock price, the BIST100 index, and the USD/TRY exchange rate.

We compared the performances of the different financial anomaly detection algorithms on Ford Otosan stock, BIST100 index, and USD/TRY exchange rate data. The models used are Isolation Forest, DBSCAN, KMeans, LOF, OneClass SVM, and Autoencoder.

The Isolation Forest model has targeted significant anomalies in Ford Otosan stock. Anomalies seem not to have any direct connection with the movement of the BIST100 Index, which remains relatively stable.

Anomalies are perhaps not directly linked to the changes in the USD/TRY exchange rate, which also clearly does not fluctuate sharply.

The DBSCAN model detected a couple of anomalies in Ford Otosan stock. The detected anomalies are similar to the Isolation Forest model since they do not coincide with movements in the BIST100 index, which seems relatively stable. Also, no dramatic change in the USD/TRY exchange rate suggests no apparent connection between the anomalies in Ford Otosan and the USD/TRY parity.

The KMeans model found many anomalies with the Ford Otosan stock. However, these do not have anything relevant regarding the BIST100 index movements. Anomalies in the Ford Otosan and anomalies in the USD/TRY exchange rate have nothing to do with each other.

The LOF model caught a couple of anomalies regarding the Ford Otosan stock. There is no direct relation between the two anomalies and the movements of the BIST100 index, nor a direct relationship with USD/TRY exchange rates.

The OneClass SVM model has detected several anomalies in Ford Otosan stock. Most anomalies are detected because of an inability to estimate movements in the BIST100 index. The detected anomalies are unrelated to USD/TRY exchange rate shifts.

The Autoencoder model could find several anomalies in Ford Otosan's stock. Found anomalies do not depend on the BIST100 index, which is very stable during periods with detected anomalies. In addition, there is no direct linkage between the anomalies in Ford Otosan and USD/TRY.

More generally, the detected anomalies in Ford Otosan stock do not relate directly to movements in the BIST100 index. In detecting anomalies in Ford Otosan stocks, anomalies found in activities involving Ford Otosan stocks are not significantly related to the movements of the BIST100 index; the results then indicate that the detected anomalies are relatively independent of general market movements represented by the BIST100 index.

Similarly, anomalies in Ford Otosan stock cannot be directly linked to the change in USD/TRY parity. The USD/TRY parity does not change significantly during these periods of stock anomalies with Ford Otosan.

Although the regression analysis results show a robust positive relationship between the three variables, the anomalies are independent. This inference suggests that although a strong correlation exists between Ford Otosan, BIST100, and USD/TRY, anomalies develop independently of this general relationship.

5. Discussion

The comparative analysis of the different algorithms for detecting anomalies in financial time series data revealed essential insights into their performance. Among all, KMeans was proven to be the best-fitting model for anomaly detection. This technique supplied high sensitivity and accuracy. KMeans was good enough to detect anomalies present in the BIST100 market. Both accuracy and efficiency were demonstrated.

The best-performing algorithms are Isolation Forest and Autoencoders. While being reasonably accurate, Isolation Forest missed many anomalies. The Autoencoder was more balanced. OneClass SVM and DBSCAN did catch a high proportion of anomalies but missed many due to their low sensitivity, while LOF missed many. These results underline the necessity of choosing a suitable algorithm dependent on the dataset characteristics and application requirements.

The study emphasized the need to establish how detected anomalies relate to market conditions. Moreover, the detected anomalies for Ford Otosan, BIST100 Index, and USD/TRY exchange rates did not relate directly to the broader markets. This independence suggests that anomalies can be detected with high precision and accuracy, but their links to broader market conditions may be more complex and less direct. More research is required to understand how and why these anomalies occur and their potential impact on typical behavioral market processes.

The financial landscape can be comprehensively understood by analyzing many financial market data, including stock prices, indices, and exchange rates. The differences in performance between algorithms across various markets emphasize the need to use a tailored approach for

each market type. The strong correlations between Ford Otosan, BIST100, and USD/TRY show that anomalies detected when these markets move together are generally independent of these general trends. This is very important for market participants: local or isolated events can trigger anomalies without putting much pressure on the more significant market trends.

Integrating machine and deep learning techniques may show better precision and efficiency in detecting anomalies. The comparison clearly shows that while many conventional machine learning techniques, such as KMeans or Isolation Forest, may have high accuracy, DL techniques, such as Autoencoders, provide an added advantage in capturing finer and more complex patterns in financial data. These combinations of ML and DL approaches can make more robust frameworks for anomaly detection.

Results from the tested models are promising, but there are some limitations. The data set contains an investigation period from October 2022 to January 2024. However, more than this may be required to consider long-term trends and seasonality in the financial markets. Future research can provide quantitative testing of a more extensive variety of algorithms with an extended analysis horizon to cover more market cycles. Interfacing with macroeconomic indicators and exogenous variables can importantly implement a holistic view of the relationship between the various kinds of anomalies and the state of the market. Future research directions should further involve tests of real-time application in live trading environments to validate how robust and practical such models may be under dynamic market conditions.

6. Conclusion

The paper presents a comparative analysis of detection algorithms of anomalies in financial time-series data. It focuses on the Ford Otosan stock, BIST100 index, and USD/TRY exchange rate. Algorithms under test include Isolation Forest, Single-Class SVM, Local Outlier Factor, LOF, DBSCAN, K-Means, and Autoencoders. This study measured accuracy, precision, recall, and F1 score.

KMeans emerged as the most effective by illustrating some good accuracy and sensitivity. Isolation Forests and autoencoders were also

effective, though with some missing anomalies. The analysis highlighted that anomalies detected in the financial markets did not always correlate directly with broader market conditions, emphasizing the complexity of financial anomaly detection.

The findings add to the knowledge of ML and DL algorithms for financial anomaly detection. The research shows the importance of selecting the right algorithm for the dataset. The study's results have practical uses in risk management and investment decisions. They help identify anomalies that might indicate market issues or opportunities.

The study had some limitations. The analysis covered a short timeframe from October 2022 to January 2024. This may not capture long-term trends and seasonal changes. The study focused on specific algorithms, possibly needing better ones. It did not consider macroeconomic indicators and other factors that affect financial markets. This limits understanding of the broader context of anomalies.

Future research should look at more algorithms and more extended periods. This would capture long-term trends and seasonal changes. Including macroeconomic indicators and other factors would give a broader picture. Testing these models in live trading environments could prove their practicality. Creating hybrid models that combine several algorithms could improve accuracy and reliability.

This study helps financial information users to understand financial anomaly detection better. It compares ML and DL algorithms in detail. The findings show the complexity of detecting anomalies in financial markets. They also show the need to choose the appropriate models for the data. A combination of different techniques looks promising for improving detection frameworks. Continuous innovation in financial data analysis can enhance market stability and lead to better investment decisions.

References

Ahmed, M., Choudhury, N., and Uddin, S. (2017). Anomaly detection on big data in financial markets. Proceedings of the 2017 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining, ASONAM 2017, 998–1001. https://doi.org/10.1145/3110025.3119402

Ahmed, M., Mahmood, A. N., and Islam, M. R. (2016). A survey of anomaly detection techniques in financial domain. Future Generation Computer Systems, 55, 278–288. https://doi.org/10.1016/J.FUTURE.2015.01.001

Al Farizi, W. S., Hidayah, I., and Rizal, M. N. (2021). Isolation Forest Based Anomaly Detection: A Systematic Literature Review. 2021 8th International Conference on Information Technology, Computer and Electrical Engineering, ICITACEE 2021, 118–122. https://doi.org/10.1109/ICITACEE53184.2021.9617498

Albu, L. L., and Lupu, R. (2020). Anomaly detection in stock market indices with neural networks. Journal of Financial Studies, 9(5), 10–23.

Au Yeung, J. F. K., Wei, Z. kai, Chan, K. Y., Lau, H. Y. K., and Yiu, K. F. C. (2020). Jump detection in financial time series using machine learning algorithms. Soft Computing, 24(3), 1789–1801. https://doi.org/10.1007/S00500-019-04006-2/TABLES/6

Bachelard, C., Chalkis, A., Fisikopoulos, V., and Tsigaridas, E. (2023). Randomized geometric tools for anomaly detection in stock markets. International Conference on Artificial Intelligence and Statistics, 9400–9416.

Braei, M., and Wagner, Dr.-I. S. (2020). Anomaly Detection in Univariate Time-series: A Survey on the State-of-the-Art. https://arxiv.org/abs/2004.00433v1

Chalapathy, R. (2019). Deep Learning for Anomaly Detection: A Survey. https://doi.org/10.48550/arxiv.1901.03407

Choi, K., Yi, J., Park, C., and Yoon, S. (2021). Deep Learning for Anomaly Detection in Time-Series Data: Review, Analysis, and Guidelines. IEEE Access, 9, 120043–120065. https://doi.org/10.1109/ACCESS. 2021. 3107975

Crépey, S., Lehdili, N., Madhar, N., and Thomas, M. (2022). Anomaly Detection in Financial Time Series by Principal Component Analysis and Neural Networks. Algorithms 2022, Vol. 15, Page 385, 15(10), 385. https://doi.org/10.3390/A15100385

cruz, R. D. l., Kinyua, J., and Mutigwe, C. (2023). Analysis of Social Media Impact on Stock Price Movements Using Machine Learning Anomaly Detection. Intelligent Automation and Soft Computing. https://doi.org/10.32604/iasc.2023.035906

da Silva Arantes, J., da Silva Arantes, M., Fröhlich, H. B., Siret, L., and Bonnard, R. (2021). A novel unsupervised method for anomaly detection in time series based on statistical features for industrial predictive maintenance. International Journal of Data Science and Analytics, 12(4), 383–404. https://doi.org/10.1007/S41060-021-00283-Z/TABLES/13

Degirmenci, A., and Karal, O. (2022). Efficient density and cluster based incremental outlier detection in data streams. Information Sciences, 607, 901–920. https://doi.org/10.1016/j.ins.2022.06.013

Dhadhania, A. (2023). Unleashing the Power of SDN and GNN for Network Anomaly Detection: State-of-the-art, Challenges, and Future Directions. Security and Privacy. https://doi.org/10.1002/spy2.337

Elmrabit, N., Zhou, F., Li, F., and Zhou, H. (2019). Evaluation of Machine Learning Algorithms for Anomaly Detection. https://figshare.le.ac.uk/articles/conference_contribution/Evaluation_of_Machine_Learning_Algorithms_for_Anomaly_Detection/12316898

Ferreira, L., and Cortez, P. (2023). AutoOC: A Python module for automated multi-objective One-Class Classification[Formula presented]. Software Impacts, 18, 100590. https://doi.org/10.1016/j.simpa.2023.100590

Foorthuis, R. (2020). Algorithmic Frameworks for the Detection of High-Density Anomalies. https://doi.org/10.1109/ssci47803.2020.9308417

Ghrib, Z., Jaziri, R., and Romdhane, R. (2020). Hybrid approach for Anomaly Detection in Time Series Data. Proceedings of the International Joint Conference on Neural Networks. https://doi.org/10.1109/IJCNN48605.2020.9207013

Guggilam, S., Zaidi, S. M. A., Chandola, V., and Patra, A. (2019). Integrated Clustering and Anomaly Detection (INCAD) for Streaming Data. https://doi.org/10.1007/978-3-030-22747-0_4

Huang, D., Mu, D., Yang, L., and Cai, X. (2018). CoDetect: Financial Fraud Detection with Anomaly Feature Detection. IEEE Access, 6, 19161–19174. https://doi.org/10.1109/ACCESS.2018.2816564

Huang, M., Bao, Q., Zhang, Y., and Feng, W. (2019). A Hybrid Algorithm for Forecasting Financial Time Series Data Based on DBSCAN and SVR. Information 2019, Vol. 10, Page 103, 10(3), 103. https://doi.org/10.3390/INFO10030103

Huet, A., Navarro, J. M., and Rossi, D. (2022). Local Evaluation of Time Series Anomaly Detection Algorithms. Proceedings of the ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, 635–645. https://doi.org/10.1145/3534678.3539339

Kulkarni, A., Mani, P., and Domeniconi, C. (2017). Network-based Anomaly Detection for Insider Trading. https://arxiv.org/abs/1702.05809v1

Lesouple, J., Baudoin, C., Spigai, M., and Tourneret, J.-Y. (2021). Generalized isolation forest for anomaly detection. Pattern Recognition Letters, 149, 109–119. https://doi.org/10.1016/J.PATREC.2021.05.022

Li, G., and Jung, J. J. (2021). Dynamic relationship identification for abnormality detection on financial time series. Pattern Recognition Letters, 145, 194–199. https://doi.org/10.1016/J.PATREC.2021.02.004

Li, G., and Jung, J. J. (2023). Deep learning for anomaly detection in multivariate time series: Approaches, applications, and challenges. Information Fusion, 91, 93–102. https://doi.org/10.1016/J.INFFUS.2022.10.008

Li, J., Izakian, H., Pedrycz, W., and Jamal, I. (2021). Clustering-based anomaly detection in multivariate time series data. Applied Soft Computing, 100, 106919. https://doi.org/10.1016/J.ASOC.2020.106919

Li, Y., Hu, X., Li, J., Du, M., and Zou, N. (2019). SpecAE: Spectral AutoEncoder for Anomaly Detection in Attributed Networks. https://doi.org/10.48550/arxiv.1908.03849

Lok, L. K., Hameed, V. A., and Rana, M. E. (2022). Hybrid Machine Learning Approach for Anomaly Detection. Indonesian Journal of Electrical Engineering and Computer Science. https://doi.org/10.11591/ijeecs.v27.i2.pp1016-1024

Lokanan, M., Tran, V., and 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/FULL/PDF

Mazarbhuiya, F. A., and Sahmoudi, M. (2023). An Intuitionistic Fuzzy Rough Set Based Classification for Anomaly Detection. https://doi.org/10.20944/preprints202303.0489.v1

Mensi, A., Franzoni, A., Tax, D. M. J., and Bicego, M. (2021). An Alternative Exploitation of Isolation Forests for Outlier Detection. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 12644, 34–44. https://doi.org/10.1007/978-3-030-73973-7_4

Monakhov, V. G., Thambawita, V., Halvorsen, P., and Riegler, M. A. (2023). GridHTM: Grid-Based Hierarchical Temporal Memory for Anomaly Detection in Videos. Sensors. https://doi.org/10.3390/s23042087

Ray, S., McEvoy, D., Aaron, S., Hickman, T.-T. T., and Wright, A. (2018). Using Statistical Anomaly Detection Models to Find Clinical Decision Support Malfunctions. Journal of the American Medical Informatics Association. https://doi.org/10.1093/jamia/ocy041

Schneider, P., and Xhafa, F. (2022). Anomaly detection: Concepts and methods. Anomaly Detection and Complex Event Processing over IoT Data Streams, 49–66. https://doi.org/10.1016/B978-0-12-823818-9.00013-4

Shah, D., Khade, S., and Pawar, S. (2021). Anomaly detection in time series data of sensex and Nifty50 with keras. 2021 International Conference on Emerging Smart Computing and Informatics, ESCI 2021, 433–438. https://doi.org/10.1109/ESCI50559.2021.9396979

Shein, W. H., Ing, N. L., and Fitrianto, A. (2022). Stock market anomaly detection: Case study of China's securities market insider trading. AIP Conference Proceedings, 2662(1), 020036. https://doi.org/10.1063/5.0109428

Shriram, S., and Sivasankar, E. (2019). Anomaly Detection on Shuttle data using Unsupervised Learning Techniques. Proceedings of 2019 International Conference on Computational Intelligence and Knowledge Economy, ICCIKE 2019, 221–225. https://doi.org/10.1109/ICCIKE47802.2019.9004325

Siegel, B. (2020). Industrial Anomaly Detection: A Comparison of Unsupervised Neural Network Architectures. IEEE Sensors Letters, 4(8). https://doi.org/10.1109/LSENS.2020.3007880

Sridhar, S., and Sanagavarapu, S. (2021). ELM-AD: Extreme Learning Machine Framework for Price and Volume Anomaly Detection in Stock Markets. 2021 International Conference on Computing and Communications Applications and Technologies, I3CAT 2021 - Proceedings, 44–51. https://doi.org/10.1109/I3CAT53310.2021.9629409

Toshniwal, A., Mahesh, K., and Jayashree, R. (2020). Overview of anomaly detection techniques in machine learning. Proceedings of the 4th International Conference on IoT in Social, Mobile, Analytics and Cloud, ISMAC 2020, 808–815. https://doi.org/10.1109/I-SMAC49090.2020.9243329

Wang, W., Lu, D., Zhou, X., Zhang, B., and Mu, J. (2013). Statistical Wavelet-Based Anomaly Detection in Big Data With Compressive Sensing. Eurasip Journal on Wireless Communications and Networking. https://doi.org/10.1186/1687-1499-2013-269

Xu, D., Wang, Y., Meng, Y., and Zhang, Z. (2018). An improved data anomaly detection method based on isolation forest. Proceedings - 2017 10th International Symposium on Computational Intelligence and Design, ISCID 2017, 2, 287–291. https://doi.org/10.1109/ISCID.2017.202

Xu, H., Pang, G., Wang, Y., and Wang, Y. (2023). Deep Isolation Forest for Anomaly Detection. IEEE Transactions on Knowledge and Data Engineering, 35(12), 12591–12604. https://doi.org/10.1109/TKDE.2023.3270293

Xu, X., Ai, X., and Meng, Z. (2023). Research on Abnormal Detection of Gas Load Based on LSTM-WGAN. https://doi.org/10.1117/12.2681623

Yang, R., Yu, L., Zhao, Y., Yu, H., Xu, G., Wu, Y., and Liu, Z. (2020). Big data analytics for financial Market volatility forecast based on support vector machine. International Journal of Information Management, 50, 452–462. https://doi.org/10.1016/J.IJINFOMGT.2019.05.027

Yu, X., Shan, C., Bian, J., Yang, X., Chen, Y., and Song, H. (2021). AdaGUM: An Adaptive Graph Updating Model-Based Anomaly Detection Method for Edge Computing Environment. Security and Communication Networks. https://doi.org/10.1155/2021/9954951

Zhang, C., Song, D., Chen, Y., Feng, X., Lumezanu, C., Cheng, W., Ni, J., Zong, B., Chen, H., and Chawla, N. V. (2019). A Deep Neural Network for Unsupervised Anomaly Detection and Diagnosis in Multivariate Time Series Data. Proceedings of the AAAI Conference on Artificial Intelligence, 33(01), 1409–1416. https://doi.org/10.1609/AAAI.V33I01.33011409

Zhang, J., Xie, Y., Pang, G., Liao, Z., Verjans, J., Li, W., Sun, Z., He, J., Li, Y., Shen, C., and Xia, Y. (2021). Viral Pneumonia Screening on Chest X-Rays Using Confidence-Aware Anomaly Detection. Ieee Transactions on Medical Imaging. https://doi.org/10.1109/tmi.2020.3040950

Zhou, Y., Ren, H., Li, Z., Wu, N., and Al-Ahmari, A. M. (2021). Anomaly detection via a combination model in time series data. Applied Intelligence, 51(7), 4874–4887. https://doi.org/10.1007/S10489-020-02041-3/TABLES/4