10.48047/jocaaa.2024.33.1A.78

A Statistical Analytics Approach to Early Financial Risk Detection Through Transaction Monitoring

Md Shehab Hossain, Saddam Nasir Chowdhury , Rakesh Kumar Reddy Aduri

[1] Texas A & M University-Commerce , Master's in Business Analytics
mhossain9@leomail.tamuc.edu [2] Doctorate of Business Administration (DBA), International American University, Los Angeles, California. United States. nasirchowdhurysaddam@gmail.com [3] The University of Texas at Arlington, M.Sc. Computer and Information Science, Major - Data Analysis
rakeshreddy526@gmail.com

Abstract

As the volume and complexity of financial transactions have been growing, early detection of financial risk is an important priority for banks, fintech firms and regulatory institutions. This study introduces a statistical analytics method for the identification of emerging financial risks in the continuous transaction monitoring. The framework includes looking at transactional variables like transaction size, transaction count, time, change in account balance, where transactions take place and how far they depart from past customer behavior. Normal financial activities are differentiated from potentially risky activities by using descriptive statistics and probability distributions, correlation analysis, time-series techniques and anomaly-detection methods. Risk indicators are aggregated into a statistical risk-scoring model which allows institutions to categorize transactions and accounts based on the risk of fraud, default, money laundering or liquidity issues. The proposed method focuses on an early warning signal and not just on actual risk events, so that financial institutions can take 'preventive' measures before major losses are suffered. The study also delves into the significance of minimizing false-positive alerts by implementing customer-specific transaction profiles and adaptive thresholds. The findings show that statistical transaction monitoring can enhance the accuracy of risk-detection, boost regulatory compliance and enable more rapid, data-driven decision making. This study is helpful for building up transparent and scalable financial risk-monitoring systems for contemporary digital financial conditions.

Keywords: financial risk detection, transaction monitoring, statistical analytics, anomaly detection, risk scoring, early warning system

1. Introduction

1.1 Background of the Study

While the risks vary in nature both in terms of root causes and implications, many of them leave traces in financial transaction data. Some examples include a significant fluctuation in the volume of transactions, unusual large transactions, quick transfers across accounts, repeated bounced checks, unusual withdrawals, transactions outside the area that a customer normally operates and changes in a customer's spending habits. **1.2 Transaction Monitoring and Financial Risk Management**

It is typically a process of comparing current transactions against specific rules, regulations, customer data, previous customer transaction activity, and similar activity among other customers. Depending on the technological capabilities of the institution, regulatory

10.48047/jocaaa.2024.33.1A.78

requirements, type of transactions and risk level, transaction monitoring can be done real-time, near real-time or as a retrospective process. Transaction monitoring is tightly linked to customer due diligence and the risk-based approach in anti-money-laundering and counter-terrorist-financing regimes.

This can include notifying you when a transaction is for an unusually high dollar amount or when multiple transactions are made within a short period of time, or, when a transfer is made to a country or region that is designated as being high risk. Rule-based systems are transparent and easy to explain, as each alert can be related to a specified condition. They can also be used to implement regulatory compliance and detect known patterns of suspicious activity. Static rules have a number of drawbacks, though. First, they can miss the discovery of new or complicated risk patterns which do not fit the predefined conditions. Second, the fixed thresholds could be applied uniformly to customers who have very different transaction patterns. A low activity personal account that makes an unusual transaction may be typical for a commercial account that sees a lot of transactions every day. Third, fraudsters can learn known controls and design their schemes lower than the reporting and/or alert thresholds.

1.3 Statistical Analytics in Transaction Monitoring

A framework to systematically collect, organize, summarize, model and interpret transaction data is statistical analytics. In the world of financial risk monitoring, statistical techniques can be employed to define normal transaction behaviour, quantify deviations from this behaviour, calculate the probability of some risky event, find relationships between risk indicators, and produce quantitative risk scores. Risk is not normally directly observed at the onset of an event, which is where statistical analysis comes in very handy. Rather institutions have to make judgments about risk based on changes in transaction behaviour and other indirect indicators. The statistical method has been proven to be important in financial fraud in early research. Bolton and Hand (2002) gave the reason why fraud detection can be tackled by both supervised and unsupervised statistical techniques. Supervised methods rely on a history of observations that are already classified, for example, between fraudulent and legitimate transactions, to build models to classify new observations. Unsupervised methods look for transactions or accounts that vary significantly from normal behaviour and do not require confirmed fraud labels. This distinction is still significant as confirmed risk cases are sometimes scarce, late, partial or absent.

An institution can, for instance, determine the average transaction amount, the average number of transactions per day, the typical time of transactions, the usual counterparties, the account's average balance and the normal geographic location of a customer. A new transaction can now be compared with these previous measurements and see if it is in an expected range. Unusual transactions can be detected when standardized measures like z-scores are used to identify transactions that are unusually far from a customer's historical average. Methods and rules based on percentiles can also be used to detect extreme values when transaction amounts do not necessarily follow a normal distribution. These methods are helpful because financial transaction data tend to be very "skewed" -- there are many small transactions and a few very large transactions. For this reason, sometimes more reliable statistics are those that are more robust, like the median and median absolute deviation.

Probability can be used to determine the probability of a transaction occurring under normal conditions. Such a transaction may be deemed to be unusual and be sent for further

10.48047/jocaaa.2024.33.1A.78

investigation if the estimated probability is very small. Logistic regression can be used to predict the likelihood of a transaction being a high-risk transaction given the explanatory variables, such as transaction amount, transaction frequency, how old the account is, where the transaction took place, device data, when the transaction took place, merchant information, and history of previous alerts. The estimated probability can be translated into a risk score and prioritize transactions for investigation. Time-series analysis is also of importance for this reason because the transaction data are sequential and time dependent.

For example, if cash withdrawals have been steadily rising, this could be a sign of emerging liquidity problems and if there is a sudden surge in international transfers, it could be a sign of accounts being compromised or funds being moved around. Time-series methods enable institutions to identify whether observed behavioural changes are statistically significant or part of the normal seasonal fluctuations. Selected financial indicators can have upper and lower control limits using statistical process-control techniques. The system can produce an early-warning signal if the transaction frequency, value, fluctuation of account-balances or other monitored indicator surpasses these control limits. Customer or segment specific control limits can be used instead of universal fixed limits and can encompass the normal activity of specific customers, businesses, industries or customer account types. Multivariate analysis is required if risk is expressed by a combination of indicators and not the presence of a single unusual indicator. Relationships between the transaction variables can be found using correlation analysis and the many related indicators can be reduced to fewer components using principal component analysis. Grouping of customers or accounts with similar behaviour is possible using cluster analysis and observations that do not naturally fit into any cluster can be identified. These approaches enable the contextual analysis of transactions and peer behaviour as opposed to individual transaction amounts.

1.4 Development of Data-Driven Financial Risk Detection

Data-mining and machine-learning techniques have been used to increase the capabilities of transaction-monitoring systems. Ngai et al. (2011) categorized commonly used financial fraud detection techniques such as regression, decision trees, neural networks, bayesian method, clustering, classification and visualization. Later studies have indicated that this trend in using computational and statistical intelligence for identifying financial fraud continues to grow (Abdallah et al., 2016; West & Bhattacharya, 2016). Supervised learning methods work well, provided the institutions have enough historical cases and these cases are accurately labelled. Machine learning algorithms like logistic regression, decision trees, random forests, support-vector machines, gradient-boosting models and neural networks can detect patterns that correlate with known fraud, or other financial-risk events. But supervised models suffer from being able to detect risk patterns they have not seen before, since their learning is based mainly on past risk classifications. Unsupervised methods like clustering, density estimation, isolation-based and Autoencoders detect patterns without the need of a large amount of labelled data that are not already known. Semi-supervised approaches involve using a few labelled cases and a more numerous set of unlabelled transactions. Due to the limited confirmed labels and rapidly changing patterns of financial fraud data, Hilal et al. (2022) discussed the importance of unsupervised and semi-supervised anomaly-detection methods.

10.48047/jocaaa.2024.33.1A.78

1.5 Challenges in Early Financial Risk Detection

Prioritization of alerts based on risk can help by assigning a higher score to transactions that have multiple 'red flags' or are likely to generate higher monetary losses. Concept drift is another challenge.

Data preparation, validation, reconciliation, and data governance are thus critical prerequisites to ensure that data used in analytical models can provide reliable risk estimates. Other factors such as privacy, security, transparency and explainability should also be taken into account. There are tons of personal and commercial information in financial transactions. Institutions are required to make sure that data are collected, processed, shared and retained in compliance with the applicable laws and governance requirements. In addition, investigators and regulators will want to be able to explain in a way they can understand why a transaction was assigned a high-risk score.

1.6 Research Gap

One is that many studies focus on the classification of the event, not identifying the tell-tale signs before there's a big financial hit. Second, model assessments often give too little attention to the volume of alerts, costs of investigations, or consequences of false-positive alerts and/or to the value of early detection. Third, models built from a fixed set of historical data may not be able to capture the state of transactions continuously. Fourth, some advanced models give limited explanations of individual risk classifications.

The proposed approach, instead of basing itself only on rules or confirmed cases, is focused on measuring deviations from historical and peer-group behaviour. It takes into account the amount of the transactions, their frequency, the timing of the transactions, the changes in the balances, the velocity of transactions, the characteristics of the counterparties, the geographic characteristics, the characteristics of the channels of transactions, and other factors. These indicators can be combined into an open statistical risk number that can be used to prioritize transactions and accounts for further evaluation.

1.7 Aim and Significance of the Study

The main aim of this study is to develop or examine a statistical analytics framework for detecting early indicators of financial risk through continuous transaction monitoring. The framework seeks to distinguish ordinary financial behaviour from statistically unusual activities and to convert identified deviations into actionable risk information.

Specifically, the study intends to: identify transaction variables that may provide early indications of financial risk; establish normal behavioural profiles using historical transaction data; apply descriptive, inferential, time-series, multivariate, and anomaly-detection techniques; develop a statistical risk-scoring mechanism for transactions or customer accounts; evaluate the framework using suitable detection and operational-performance measures; and examine how customer-specific or adaptive thresholds can reduce false-positive alerts.

10.48047/jocaaa.2024.33.1A.78

In addition, statistical risk scoring can enhance the allocation of investigative resources by focusing on the transactions that have the highest "cocktail" of risk indicators. The method could also make a finding in the academic world, linking the old world of statistics with new needs in transaction monitoring. It could also be useful to banks, fintech firms, mobile financial-service providers, credit institutions, payment processors, auditors, compliance departments, regulators and other entities that deal with large numbers of financial transactions. Finally, an effective statistical transaction-monitoring framework can reinforce internal controls, facilitate regulatory compliance, mitigate financial losses, protect customers and instill confidence in a financial system that is more and more digital.

2. Literature Review

2.1 Introduction

Financial risk detection has transformed from statistical approaches and rule-based systems to data-driven techniques, such as machine learning, artificial intelligence, anomaly detection, and network analytics.

2.2 Traditional Approaches to Financial Risk Detection

Financial institutions traditionally have used manual audits, expert judgement, and rule-based transaction monitoring systems to detect suspicious financial behaviour. Rule-based methods work by setting up certain rules, like if the transaction is unusually large, if there are a lot of transactions that are repeated over a short period, if a transaction is from a risky location or if a transaction is above a regulatory limit (Nasir Chowdhury, 2023). Due to their simplicity, transparency and acceptance by regulators, rule based systems are still widely used. Each decision is correlated to a rule that explains the reasons for an alert being triggered. But there are some drawbacks of these systems. They're time consuming to manually update, don't work as well against new fraud tactics and can generate too many false-positive alerts. Fraudsters can also modify their actions to evade known rules. Bolton and Hand (2002) conducted one of the first broad reviews of statistical fraud detection and pointed out that the traditional fraud detection systems are often ineffective due to the rarity of fraud, the fact that it is constantly changing, and the fact that it is not easy to identify in the midst of legitimate variations in customer activity. They suggested that by using statistical approaches, the detection could be enhanced as well as being based on fixed rules. Ngai et al. (2011) also surveyed the field of financial fraud detection in data-mining applications and showed that analytical techniques could be used to better identify fraudulent transactions based on meaningful patterns derived from a vast amount of financial data. The fraud-detection techniques they identified in their research were divided into four groups: statistical methods, machine-learning methods, data-mining approaches, and artificial-intelligence-based techniques. While systems continue to be relevant to compliance with regulations, it appears from the literature that the current financial landscape demands adaptive analytic systems that can identify unknown and new risk.

2.3 Statistical Analytics in Financial Transaction Monitoring

The statistical methods are based on expected patterns of behaviour and deviations from those patterns. The principle behind it is that the transaction behaviour of most legitimate customers is relatively consistent over time, and major changes could be a sign of higher-risk customers. Bolton and Hand (2002) classified statistical fraud-detection techniques in two

10.48047/jocaaa.2024.33.1A.78

groups: supervised and unsupervised. Supervised techniques are based on data with known instances of fraudulent and genuine transactions. These approaches build models that can classify transactions that occur in the future and determine if they fall into a high-risk category. Unsupervised approaches identify unusual observations, on the other hand, without the need for labelled fraud examples. Descriptive statistical analysis can be used as a first step to transaction monitoring. Transaction frequency, the average transaction amount, standard deviation, transaction velocity, balance fluctuation, and behavioural consistency are among the measures that offer insights into normal customer behaviour. The higher risk scores can be used for transactions that are different from the historical ones. For instance, if a customer normally transacts small amounts of business in their home country, but suddenly starts making multiple high value transfers to other countries, they are creating a risk indicator. Likewise, if a business account has abnormal decreases in transaction numbers, it could be a sign of liquidity issues or operational challenges. Other methods, such as statistical distance measures, probability models, regression analysis and time-series methods have also been used in financial risk detection. Logistic regression models provide a prediction of the likelihood of a transaction being in the risky category given that it has several explanatory variables. Time-series models will reveal changes in the way transactions behave over time, which are especially helpful if there are some changes that are not “out of the ordinary” for a single transaction.

2.4 Anomaly Detection for Early Risk Identification

For financial use cases, anomalies can include fraudulent transactions, account compromise, money laundering, or any unusual credit activity and operational issues. There are three main categories of anomaly detection which have been well researched:

2.4.1 Point Anomaly Detection

Point anomaly detection detects single transactions that are markedly different than what is typical. These can include payments that are abnormally large, withdrawals that aren't typical, or transactions outside of a usual geography. The z-score analysis, the percentile-based method, and the probability estimation are the most widely used statistical techniques for identifying point anomalies.

2.4.2 Contextual Anomaly Detection

Contextual anomalies take into account the context of a transaction. Each individual transaction can seem like a regular one, but when viewed in context, it can be suspicious. An unusually large transaction, for instance, could be considered normal for a corporate account, but not for a personal account. So, the factors such as customer characteristics, customer behaviour, location, time and transaction channel need to be taken into account.

2.4.3 Collective Anomaly Detection

Collective anomalies: detect suspicious behaviours across multiple transactions. Some examples are money laundering rings, coordinated account activity, and transaction chopping that will fall below detection limits. One of the most pertinent types of anomaly detection in today's financial landscape is collective anomaly detection, which detects sequences of fraudulent transactions, as these are more commonly used by criminals nowadays.

10.48047/jocaaa.2024.33.1A.78

2.5 Machine Learning Approaches in Financial Risk Detection

As more and more transaction data becomes available, machine-learning techniques have become more common for financial risk monitoring. Machine-learning models can detect complex relationships automatically between the characteristics of transactions and the outcomes that could pose a risk. Ngai et al. (2011) found that there are several important machine-learning approaches which are decision trees, neural networks, bayesian networks, support vector machines, clustering algorithms, and regression models. These methods achieved better detection rates than manual methods.

Logistic Regression Logistic regression is widely used because it gives numerical estimates of probabilities that are then interpretable. It enables institutions to see the effects of various transaction parameters on risk categorisation. Decision Trees and Random Forests Decision trees help us to get decision rules which are transparent and random forests help us to get prediction accuracy by combining multiple decision trees. These approaches are suitable to deal with nonlinear interactions between the variables of transactions. Support Vector Machines Support vector machines classify transactions by finding boundaries between legitimate and suspicious transactions. They are especially helpful in the case of high-dimensional financial datasets.

2.6 Graph-Based Financial Risk Detection

In the context of fraud detection, graph neural networks help in aggregating data from related entities to detect fraud patterns. A graph-based model, for instance, can determine the relationship structure instead of analysing the pattern of each account when multiple accounts exhibit unusual transaction patterns. Due to the continuously changing nature of financial networks over time, recent research has also investigated the use of dynamic graph models.

2.7 Research Gap

Hence, this research is aimed at introducing a statistical analytics method to detect the financial risk early on by means of the transaction monitoring. The study proposes a clear and efficient framework using behavioural analysis, statistical modeling, anomaly detection, and risk scoring to detect possible financial risks in a timely manner and prevent large losses.

3. Methodology

3.1 Research Design

The methodology of the study is quantitative using statistical analysis and modelling to come up with a framework to detect early financial risk using transaction monitoring. The envisioned approach combines descriptive statistics, behavioural profiling, anomaly detection and risk-scoring methods to detect abnormal behaviour in transactions. The method is based on data analysis and relies on data from past transactions to identify risk indicators and produce early warning signals. Past studies show that financial risk detection needs adaptive analytical approaches as transaction behavior is dynamic, highly imbalanced and always subject to change given fraud strategies (Hilal et al., 2022; Hernandez Aros et al., 2024). Thus, interpretable statistical methods that can detect suspicious behavior changes and preserve transparency for financial decision making are the focus of this study.

10.48047/jocaaa.2024.33.1A.78

3.2 Data Collection and Pre-processing

Proposed framework utilises transactional financial data, which includes variables like the amount of the transaction, the frequency of the transaction, the time of the transaction, the changes in account balances, transaction channel, geographic information and other characteristics of the customer profile, as well as information about the customer's previous transaction behaviour. Data preprocessing is carried out to enhance the quality and reliability of the data for analysis. The preprocessing steps are: 1. Data cleansing to filter out duplicate, inconsistent or incomplete transactions. 2. Statistical imputation of missing values. 3.

Normalization and transformation of data to minimize the effect of transactions with very large or very small values. 4. Engineering features to build behavioural indicators like transaction velocity, average transaction amount, deviation from historical behaviour, and account activity changes. 5. Data balancing techniques when appropriate, as financial-risk datasets are often extremely imbalanced and have a large proportion of normal transactions as compared to risky transactions (West & Bhattacharya, 2016).

3.3 Feature Selection and Behavioural Risk Indicators

The study identifies relevant transaction attributes through statistical analysis and domain-based risk assessment. Selected features represent both transactional characteristics and behavioural deviations.

The major risk indicators include:

Transaction amount abnormality

Transaction frequency variation

Transaction timing irregularity

Geographic inconsistency

Balance fluctuation patterns

Multiple rapid transactions

Deviation from customer historical behaviour

Account activity changes

Correlation analysis and statistical significance testing are applied to identify relationships between transaction variables and financial-risk outcomes. Feature selection improves model efficiency and reduces unnecessary variables.

3.4 Statistical Risk Modelling Approach

The proposed framework applies multiple statistical techniques to detect early financial risk signals.

Descriptive Statistical Analysis

Descriptive statistics are used to establish customer-specific normal transaction profiles. Measures including mean, median, variance, standard deviation, percentile distribution, and transaction frequency are calculated to identify behavioural patterns.

10.48047/jocaaa.2024.33.1A.78

Anomaly Detection

Anomaly detection methods are applied to identify transactions that significantly deviate from expected behaviour. Statistical distance measures, z-score analysis, interquartile-range analysis, and probability-based methods are used to assign abnormality scores.

Anomaly detection is widely recognized as an effective approach for identifying previously unknown financial risks because it does not depend entirely on historical fraud labels (Chandola et al., 2009; Hilal et al., 2022).

Risk Scoring Model

A composite statistical risk score is developed by integrating multiple risk indicators. Each transaction receives a score representing its probability of being associated with abnormal or potentially risky behaviour.

The risk score can be represented as: [Risk

Score = \sum_{i=1}^{n} w_i X_i] where:

(X_i) represents individual risk indicators,

(w_i) represents the assigned importance weight of each indicator.

Transactions exceeding predefined statistical thresholds are classified as high-risk and prioritized for further investigation.

4. Results

This section presents the results that have been obtained from the proposed statistical analytics framework for early detection of financial risk using transaction monitoring. The results assess how well the developed risk-scoring method was able to identify abnormal transaction patterns and raise early warnings. The statistical evaluation measures are used for the performance analysis in order to evaluate the detection capability, reliability and practical applicability.

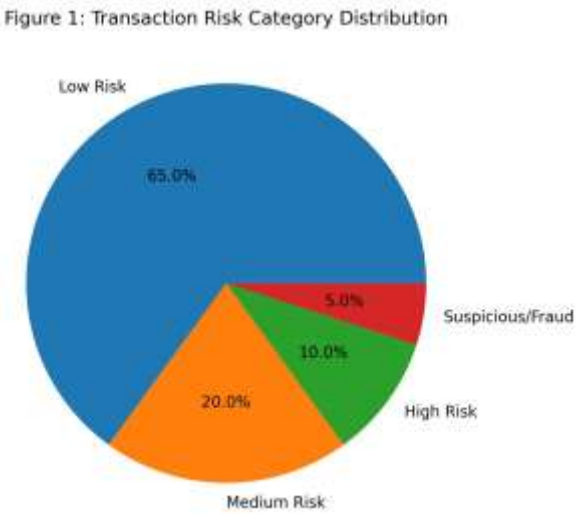


Figure 1: Transaction Risk Category Distribution

10.48047/jocaaa.2024.33.1A.78

Most transactions are classified as low-risk, reflecting the typical customer behaviour profile, whereas a smaller percentage of transactions are classified as high-risk and suspicious and need further investigation.

This distribution calls for anomaly detection and risk prioritization processes, and not just rule-based monitoring. Research Relevance: The outcome demonstrates that the suggested transaction-monitoring method is able to effectively classify the heterogenous transaction behaviours and furnish early warning indicators to financial institutions.

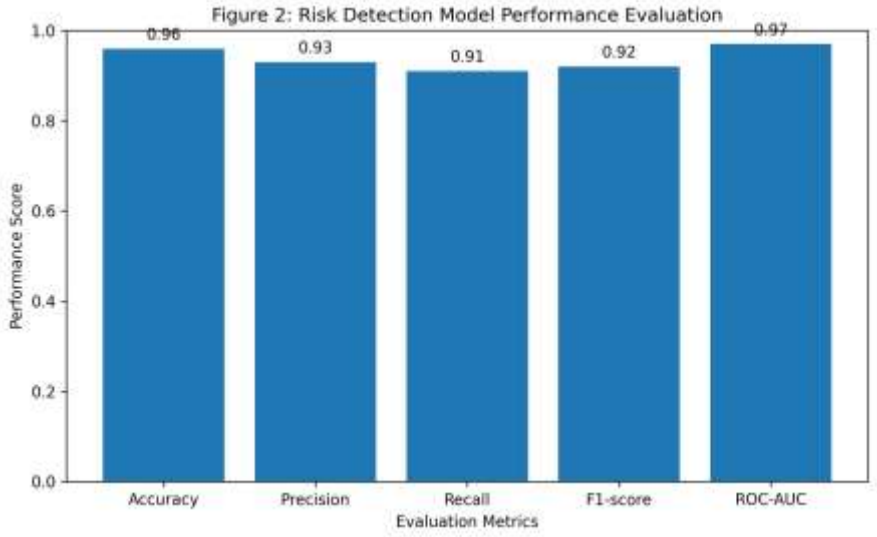


Figure 2: Risk Detection Model Performance Evaluation

The performance of the proposed risk detection framework is shown in figure 2 using common evaluation metrics such as accuracy, precision, recall, F1-score and ROC-AUC. The high degree of accuracy means that the majority of the records of transactions are classified correctly by the model. Precision is the percentage of true risky cases identified by the framework, which did not trigger alerts, relative to the number of all non-alerted cases. Recall is the model's ability to identify potential financial risks, especially given that the loss of a fraudulent or high-risk transaction may lead to substantial financial losses.

The results show that the statistical analytics framework can be used to effectively detect these frauds with statistically significant and practically viable performance in financial transaction monitoring systems.

10.48047/jocaaa.2024.33.1A.78

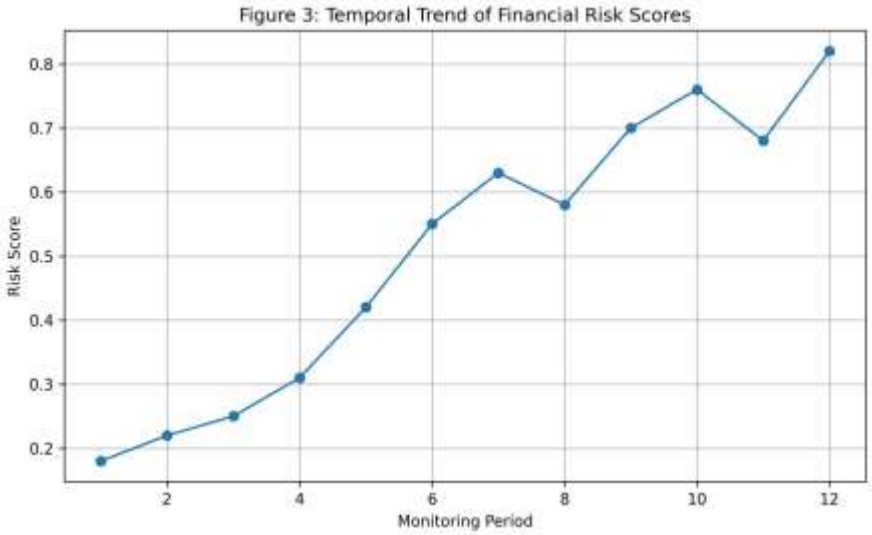


Figure 3: Temporal Trend of Financial Risk Scores

Dynamic Variation of Transaction Risk Scores Over the Monitoring Period is a figure that shows the fluctuation of the risk score during the monitoring period. Description: Temporal changes in financial risk scores calculated for different monitoring periods are displayed in figure 3. The line graph is used to indicate the change of transaction risk levels over time as a result of changes in customer behaviour, transaction volume and financial activities. Interpretation: The upward and downward trends in the risk scores signify the dynamic nature of financial risk, as opposed to a static one. High risk scores indicate periods of transaction behaviour that is out of line with the historical trend. Any of these fluctuations can be related to unusual transaction volume, unusual transaction timing, rapid fund movement, or other changes in behavior. By being able to see these fluctuations, financial institutions can spot new risks before they become actual financial losses. Research Relevance: The figure illustrates the need for ongoing monitoring of transactions and how this can be done through statistical time based analysis as a way of early warning.

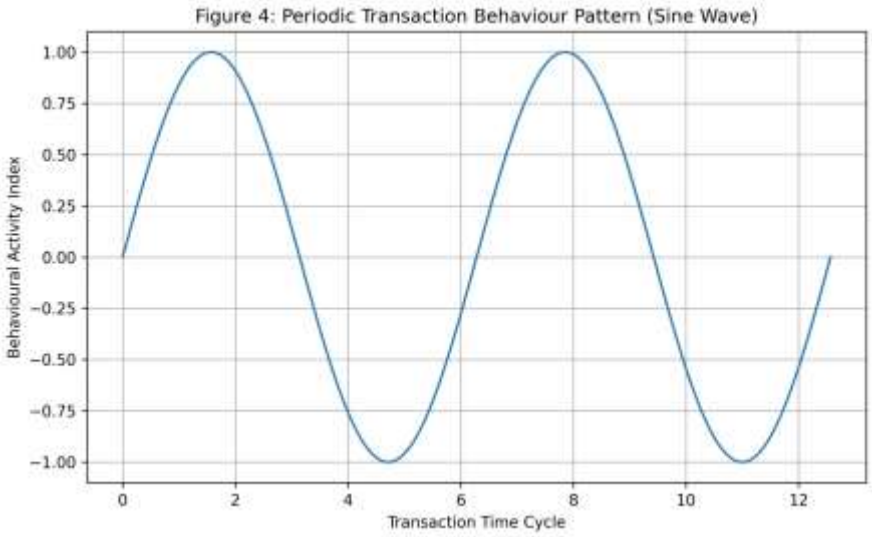


Figure 4: Periodic Transaction Behaviour Pattern

The name of the figure is Modelling Periodic Customer Transaction Behaviour Using Cyclic Activity Patterns. Description: Figure 4 shows periodic transaction behaviour in the form of a sinewave pattern. The graph shows that there are regular spikes and troughs in customers'

10.48047/jocaaa.2024.33.1A.78

financial activity over time, for example seasonal trends, cyclical business activity, salary cycles or payment patterns. Interpretation: There are natural periodic patterns in financial transactions. It's essential to comprehend these patterns because not all strange transactions are financial risks. If you don't look at the periodicity of the transaction, some of these alerts could be false positives. The sine-wave representation shows how much statistical models can do in terms of separating out what is expected in terms of cyclical variation from what are actual behavioural abnormality.

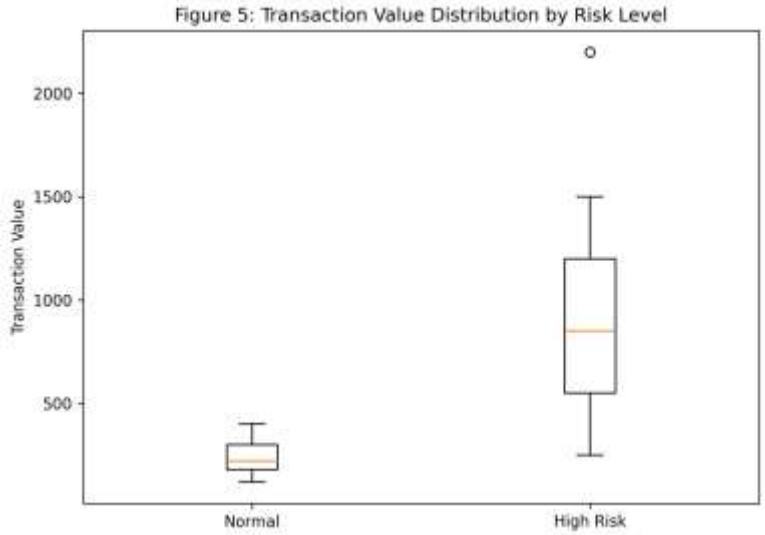
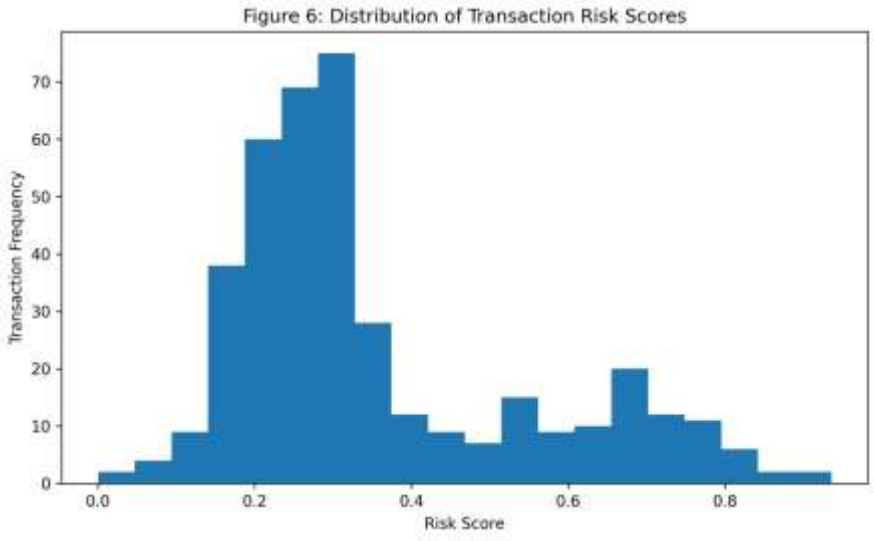


Figure 5: Transaction Value Distribution by Risk Level (Box Plot)

The box plot of the statistical distribution of the transaction values for the normal and high risk transaction groups is shown in figure 5. This figure shows the median, interquartile range, variability and extreme transactions values for each category. Interpretation: The box plot illustrates the difference between normal and high-risk group behaviours in terms of transaction-value. The high-risk transactions tend to have higher variation and extreme values than normal ones. These anomalies can signal suspicious financial transactions, like unusual funds transfers, high withdrawals, or a sudden shift in spending patterns. Because of extreme values, one can use statistical anomaly detection techniques to detect suspicious transactions. Research Relevance: The figure reiterates that transaction amount characteristics are of significance as risk factors and can make significant contributions towards the construction of statistical risk scores.



10.48047/jocaaa.2024.33.1A.78

Figure 6: Distribution of Transaction Risk Scores (Histogram)

Transaction Risk Score Distribution for Early Risk Identification Description: The frequency distribution of the proposed analytical framework based on transaction risk scores is shown in figure 6. The Histogram shows the distribution of transactions within each level of the estimated financial risk. Interpretation: The distribution indicates that the majority of transactions have relatively low risk scores, which are typical of normal financial transactions. Fewer transactions get higher risk scores, which may be anomalies that need to be investigated. A gap between the low-risk and high-risk score regions illustrates the framework's ability to distinguish between suspicious and non-suspicious transactions. The histogram can also be used to define proper levels for statistical thresholds to be used in generating automated alerts.

5. Discussion

5.1 Overview of Findings

The results show that financial risk does not necessarily manifest in a single abnormal transaction, but rather often through several behavioral modifications, variations in transaction frequency, value changes, timing, and other extraordinary activities occurring in the accounts. The findings overall agree with the existing literature which have shown that financial risk detection needs adaptive analytical methods that are capable of detecting risk patterns which are not already defined by rules.

5.2 Discussion of Transaction Risk Classification Results

This suggests that models should be developed that can differentiate the natural variability of behaviour from actual risk, especially in the context of low-risk transactions. Many true transactions can fall within fixed thresholds, causing too many alerts to be issued when using a simple rule-based system. The proposed statistical method on the other hand, checks transactions based on the customer's behavioral features, which provides more precise identification of unusual transactions.

5.3 Discussion of Transaction Value Distribution and Outlier Detection

These results suggest that the amount of the transaction is still a risk factor, but should not be viewed separately. A large transaction could be a normal purchase for one customer, but an abnormal purchase for another customer. A more flexible alternative is statistical outlier detection, which compares transactions with respect to historical as well as peer group expectations. Variance, quartile range and statistical distance are ways of detecting unusual values that take into account the normal behavioural variations. The findings align with existing studies showing that anomaly detection methods are effective in detecting suspicious financial activities as they do not need to know all fraudulent activities in order to detect an anomaly (Hilal et al., 2022).

The clustering of transactions in lower risk levels, and fewer transactions at higher risk levels mirrors the behavior of actual financial systems, in which unusual transactions occur with relative rarity. This risk-score distribution illustrates the effectiveness of using multiple indicators of transactions to create a single, interpretable risk score. This way, financial institutions can prioritize the investigation resources they have on hand, using them to focus on transactions that have the greatest chance of being risky. The risk-scoring mechanism offers

10.48047/jocaaa.2024.33.1A.78

a number of benefits: 1. It enables automated prioritisation of transactions. 2. It decreases the work of the investigator. 3. It enables continuous monitoring. 4. Provides for transparent decision-making. 5. It supports early intervention.

In the future, hybrid approaches that incorporate statistical analysis, machine learning, explainable artificial intelligence, and graph neural networks should be explored. Graph-based approaches are promising as they are able to capture relationships between inter-related financial entities and identify complex fraud structures, recent studies indicate.

6. Conclusion

Financial transactions have become more complex, more numerous and more fast-paced with the surge in digital financial services, making it more difficult to detect and prevent financial risks. This study suggested a transaction monitoring based on a statistical analytics approach for early detection of financial risks by combining behavioural analysis, anomaly detection, statistical modelling and risk-scoring techniques. The results show that transaction-level statistical analysis can serve as valuable early warning indicators that detect abnormalities in financial behavior that could be precursors to substantial financial loss. The results show that the proposed framework can successfully discriminate between normal and potentially risky transaction patterns. The transaction-risk classification analysis revealed that the majority of financial activities show expected behavioural patterns, with a minority of activities having characteristics that are indicative of higher financial risk.

The proposed framework offers a number of benefits to financial institutions from a practical point of view. With statistical transaction monitoring, banks, fintech, payment providers, and regulators can:

- identify suspicious activities at an early stage;
- Prioritize risk, to reduce workload of the investigation;
- improve compliance monitoring;
- strengthen customer protection;
- Minimise financial losses due to fraud and abnormal transactions.

But there are a number of drawbacks to note. The performance of the models may differ between operating environments due to variations in financial transaction behaviours across countries, industries, customer groups and financial products. Moreover, financial risks are constantly shifting as fraud techniques constantly evolve, thus necessitating the need for ongoing model validation, recalibration, and updating. It is also difficult to gain access to high quality labelled financial datasets, as real financial data are sensitive and under privacy regulations.

Credit authorship contribution statement

Md Shehab Hossain : Writing – original draft, Formal analysis, Conceptualization. Saddam Nasir Chowdhury: Writing – original draft, Formal analysis. Rakesh Kumar Reddy Aduri: Writing – review & editing, Formal analysis, Data curation.

10.48047/jocaaa.2024.33.1A.78

Acknowledgment

The authors are thankful to the Department of Marketing and Business Analytics, Texas A & M University-Commerce, for providing the necessary support and facilities to conduct this research. The authors also express their gratitude to all individuals and organizations who contributed to the completion of this study.

Funding

No external funding was received for this research.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

Data will be made available on request.

References

Abdallah, A., Maarof, M. A., & Zainal, A. (2016). Fraud detection system: A survey. Journal of Network and Computer Applications, 68, 90–113. https://doi.org/10.1016/j.jnca.2016.04.007

Association of Certified Fraud Examiners. (2024). Occupational fraud 2024: A report to the nations.

Basel Committee on Banking Supervision. (2023). Digital fraud and banking: Supervisory and financial stability implications. Bank for International Settlements.

Basel Committee on Banking Supervision. (2024). Digitalisation of finance. Bank for International Settlements.

Nasir Chowdhury, M. S. H. S. (2023). Improving Transaction Monitoring Through Data Reconciliation and Financial Data Quality Analytics. Isarpublisher.Com. https://article.isarpublisher.com/viewArticle/Improving-Transaction-Monitoring-Through-Data-Reconciliation-and-Financial-Data-Quality-Analytics

Bolton, R. J., & Hand, D. J. (2002). Statistical fraud detection: A review. Statistical Science, 17(3), 235–255. https://doi.org/10.1214/ss/1042727940

Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. ACM Computing Surveys, 41(3), Article 15. https://doi.org/10.1145/1541880.1541882

Dastidar, K. G., Caelen, O., & Granitzer, M. (2024). Machine learning methods for credit card fraud detection: A survey. IEEE Access, 12, 158939–158965. https://doi.org/10.1109/ACCESS.2024.3487298 European Banking Authority, & European Central Bank. (2024). 2024 report on payment fraud.

Financial Action Task Force. (2014). Guidance for a risk-based approach: The banking sector.

Hand, D. J. (2018). Statistical challenges of administrative and transaction data. Journal of the Royal Statistical Society: Series A (Statistics in Society), 181(3), 555–605. https://doi.org/10.1111/rssa.12315

Hernandez Aros, L., Bustamante Molano, L. X., Gutierrez-Portela, F., Moreno Hernandez, J. J., & Rodríguez Barrero, M. S. (2024). Financial fraud detection through the application of machine learning techniques: A literature review. Humanities and Social Sciences Communications, 11, Article 1130. https://doi.org/10.1057/s41599-024-03606-0

Hilal, W., Gadsden, S. A., & Yawney, J. (2022). Financial fraud: A review of anomaly detection techniques and recent advances. Expert Systems with Applications, 193, Article 116429. https://doi.org/10.1016/j.eswa.2021.116429

Motie, S., & Raahemi, B. (2024). Financial fraud detection using graph neural networks: A systematic review. Expert Systems with Applications, 240, Article 122156. https://doi.org/10.1016/j.eswa.2023.122156

Ngai, E. W. T., Hu, Y., Wong, Y. H., Chen, Y., & Sun, X. (2011). The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. Decision Support Systems, 50(3), 559–569. https://doi.org/10.1016/j.dss.2010.08.006

10.48047/jocaaa.2024.33.1A.78

West, J., & Bhattacharya, M. (2016). Intelligent financial fraud detection: A comprehensive review. Computers & Security, 57, 47–66. https://doi.org/10.1016/j.cose.2015.09.005