Comprehensive Journal of Science
Volume (10), Issue (37), (NOV. 2025)
SICST2025, www.sicst.ly
ISSN: 3014-6266

مجلة العلوم الشاملة
عدد خاص بالمؤتمر الدولي الثالث للعلوم والتقنية
المجلد (10)، العدد (37)، (نوفمبر2025)
ردمد: 3014-6266

Early Prediction of Banking Closure Failures Using Machine Learning for Anomaly Detection

Abdulgader Abogila , Dr. Juma Ibrahim
[1,2] Postgraduate office, software development technology, Collage of Computer Technology Tripoli (CCTT)
Tripoli, Libya
Corresponding author: aa2303010@cctt.edu.ly
Corresponding author: juma.ibrahim@cctt.edu.ly

التنبؤ المبكر بفشل إغلاق البنوك باستخدام التعلم الآلي للكشف عن الشذوذ

عبدالقادر ابوقيلة، د. جمعة إبراهيم
مكتب الدراسات العليا، قسم هندسه تطوير البرمجيات، كليه تقنيه الحاسوب طرابلس، ليبيا

Received: 30-09-2025; Revised: 10-10-2025; Accepted: 31-10-2025; Published: 25-11-2025

Abstract

Closing the banking system is one of the most crucial things that should be done in financial institutions especially banks. This can happen daily, monthly, or yearly. When the bank follows a proper routine every day, it helps maintain consistency in its operations, and it will also help maintain the internal and external balance of the bank. The closing is stopped and delayed when any mistake or unusual and suspicious transaction occurs. Thus, it adds stress, work, and effort. This raises the dangers of doing business. Banks must close every day to deal with the large number of transactions that happen during the day that the bank's actual activities to directly find any mistakes, suspicions, fraud attempts or theft. Unlike the shops or stores that are mostly closed for a day in the month or a year, this is different. The research proposes a Machine Learning based approach for the early identification of anomalies leading to daily closing failure. We used synthetic data that acted like a real bank setting. The dataset used was open-source and available on Kaggle as well. They used several models such as Random Forest, which is a supervised model, and Isolation Forest, which is an unsupervised model The models were deployed and analyzed on performance through metrics pertaining to machine learning such as recall, positive accuracy, F1-Score, and ROC-AUC. The study showed the results of Random Forest model are highly accurate for classifies data. The model called Isolation Forest was also quite capable of finding the unexpected patterns. The applications of both models together could be beneficial in developing and constructing a model for an early warning system which would reduce sudden closures and enhance the role of digital transformation in the banking industry as a whole.

Keywords:
Banking Systems, Daily Closure, Machine Learning, Anomaly Detection, Synthetic Data, Random Forest, Isolation Forest.

الملخص

في المؤسسات المالية، وخاصةً المصارف، يُعدّ إغلاق النظام المصرفي من أهمّ الإجراءات الواجب اتخاذها، سواءً كان إغلاقًا يوميًا أو شهريًا أو سنويًا. تضمن عملية الإغلاق اليومي الناجحة اتساق عمليات البنك وتحمي أرصدته الداخلية والخارجية. أي خطأ أو معاملة غير طبيعية أو مشبوهة تُعطّل عملية الإغلاق، مما يُولّد ضغطًا وجهدًا إضافيين. وهذا يزيد من المخاطر التشغيلية. بخلاف الأنشطة التجارية الأخرى، كالمتاجر وغيرها، التي تقتصر على الإغلاقات الشهرية أو السنوية، يُطلب من المصارف إجراء

إغلاقات يومية لمعالجة الحجم الكبير من المعاملات التي تحدث خلال اليوم، وللكشف المباشر عن أي أخطاء أو شكوك أو محاولات احتيال أو سرقة. في هذا البحث، نقترح نموذجًا قائمًا على تقنيات التعلم الآلي للكشف المبكر عن الحالات الشاذة التي تُسبب فشل الإغلاق اليومي. اعتمدنا على بيانات تركيبية تُحاكي بيئة مصرفية حقيقية. بالإضافة إلى ذلك، استفدنا من مجموعة بيانات مفتوحة المصدر متاحة على منصة Kaggle. طُبّقت نماذج مُختلفة، بما في ذلك نموذج الغابة العشوائية (نموذج مُراقَب) ونموذج الغابة المعزولة (نموذج غير مُراقَب). تم تطبيق هذه النماذج وتقييم أدائها باستخدام مجموعة من المؤشرات المستخدمة في التعلم الآلي، مثل التذكر، والدقة الإيجابية، ودرجة F1، ومساحة المنطقة تحت المنحنى (ROC–AUC). أظهرت النتائج أن نموذج الغابة العشوائية حقق معدلات دقة عالية عند التعامل مع البيانات المصنفة. كما تميز نموذج الغابة المعزولة بقدرته على اكتشاف الأنماط غير المتوقعة. أظهرت هذه التطبيقات أن دمج النموذجين يمكن أن يشكل أساسًا لتطوير وتصميم نموذج نظام إنذار مبكر من شأنه أن يساعد في الحد من الإغلاقات المفاجئة، ويعزز دور التحول الرقمي في القطاع المصرفي بشكل عام.

الكلمات المفتاحية: الأنظمة المصرفية، الإغلاق اليومي، التعلم الآلي، اكتشاف الشذوذ، البيانات الاصطناعية، الغابة العشوائية، غابة العزلة.

Introduction

Banks face difficulty ensuring daily closure of their banking systems. The banking system's closure process happens daily when the above internal and external accounts do not match at the end of each working day. This keeps balances accurate and data safe. When the daily closing is done properly, mistakes or discrepancies are discovered early. Even little mistakes can lead to quick fixes when paired with reporting errors and other problems. If banks do not shut down on a regular basis on a daily basis, it causes too many mistakes to happen. Moreover, business goes on more in a disciplined and orderly way.

If any transactions get flagged as wrong, unusual, or suspicious, it could slow down closing and put additional strain on staff and additional work effort, and increase the bank’s operating risks (Petropoulos et al, 2020). Many surveys suggest that medium and large financial institutions struggle to keep their financial records accurate (Ranjan, 2025). This can cause lost revenue and a higher risk of fraud. The gaps in the settlement process can lead to the violation of generated rules by banks, delays in review and audit processes, and weakness in operational management. Due to the concerns regarding NPA and money laundering, daily closing is adopted as a means to mitigate these risks (Rachmad, 2025).

Banks need to shutter accounts daily. Other businesses, like a store, shop, workshop, service office and other non-financial companies do it once a month, once a quarter, once in six months or once a year. The reason for this is that we have a lot of different transactions taking place in a single day. So, it becomes crucial to identify any mistakes, doubts, oddities, or fraudulent efforts straightaway, before they happen. In banks with lots of transactions every day, closing every day is essential to track rapid cash transactions, adhere to the rules and keep the customer happy. Financial control teams can catch fraud in time by comparing internal records with external sources to find discrepancies (Chohan, 2025). These are done on a daily basis by movie reconciliation of the business. This allows for locating issues (such duplicate entries, unapproved withdrawals, or unfinished transactions) and taking the right steps before any loss accumulation. Daily close of business, regularly, helps the bank keep its records clean and updated in compliance with the rules so that the bank is always ready to fulfill audit and compliance requirements. If daily closing process does not take place for any reason, apart from being malfunctioning, it can also indicate a strange act or a security breach. For example, an unusual transaction as a result of cyberattack or technical failure which remains undetected and unfixed for a while can damage the financial system considerably and weaken its stability. It's like looking for a needle in a haystack because there are so many transactions and so few real anomalies. We need tools that can monitor and perform automated analysis of large amounts of data in real time so as to catch them early and prevent them from causing problems. The banking and finance sector has recently discovered artificial intelligence and machine learning technologies as a feasible solution to such problems. Many banks all over the world have showcased powerful anomaly detection tools capable of identifying fraud, combating money laundering, and other illicit activities. As time passes, more people are realizing the importance of smart financial data analysis. This means that machine learning models can quickly identify and report unusual patterns in transaction flow. These programs are effective against financial fraud and are being assessed for application in monitoring key internal banking functions, including the daily closing of accounts.

Our paper proposes a new model using implemented machined learning approaches to detect abnormalities which could affect daily closure in banks. In order to do this, synthetic data mimicking the real banking environment was used to ensure that a multitude of conceivable scenarios were addressed. Using an open data set of Kaggle in this model increased its accuracy and realism. Various machine learning models were adopted for validation and comparison purposes. The Random Forest model is a supervised learning technique that makes use of labelled data, whereas the Isolation Forest model is an unsupervised learning technique that detects anomalies that does not need labelled data. When we combine these two methods, we can handle these two situations. On one hand, we can handle basis historical data with identifiable failures. On the other hand, we can handle fresh, unknown anomalies. To evaluate the performance of the models, we used a few machine learning metrics. The basic metrics included recall, precision, F1 score and area under the ROC curve (ROC-AUC). The experiments showed that the Random Forest model performed better than the Classification Model based on getting high accuracy rates from the labeled data. The Segregated Forest model was better in finding surprising patterns in unlabeled data. The results show that creating a dual approach that mixes supervised and unsupervised learning is vital for performing anomaly detection. The unification of the two models creates solid scheme for an early-warning system which forecasts closure failures before they occur and thus prevents the abrupt closure failures that disrupt operation of banks. In addition, this strategy highlights the importance of digital transformation to ensure the stability of the banking business and enhance the efficiency of operational risk management in the financial sector.

Problem Statement

Being a bank, the accuracy and speed of daily closing procedures are vital. Because they ensure that the transactions have been settled correctly and that the internal accounts of the bank match the external one. But this process still has a lot of operational risks. It is possible that a mistake of entering the same information twice, not entering a transaction or entering the wrong amount will throw the whole cycle.

In practice, the system only detects the error when it reaches the defective data point, which means that useful hours of work are lost before the closing process is deemed a failure. For instance, if a large number of reports are processed and a failure occurs later in the sequence then the entire workflow has to be restarted which delays financial reporting and adds pressure on the IT infrastructure and financial resources team. Many of today's work methods are reactive.

This means traditional rule-based checking and manual auditing find problems only after they occur. This raises operational risks and reduces the reliability of financial data. This kind of reaction can causes banks to have disruptions at their daily operations. It may sometimes make them non-compliant with the regulator. There's a need for solutions that prevent failure scenarios that stall the closing process. These issues impact a bank's bottom line. Machine learning technologies enable analysis of huge volume of transaction data and early detection of aberrant patterns, which is a promising solution to reduce the unexpected disruptions and enhance resilience and operational efficiency in the banking sector significantly..

Literature review

In recent years, the banking and finance sectors have witnessed a significant increase in the use of Artificial Intelligence (AI) and Machine Learning (ML) technologies (Armutcu, 2025). Financial technologies can speed up the closing, and find fraud, and other issues in the data (Shang et al, 2025). Recently, several studies examined this issue from different angles. Farouk (2025) discussed the future of closing processes. The closing procedure can be expedited with the use of technology such as AI and ML, allowing for increased accuracy of data and control measures. This research focused on the role of automation in simplifying closure operations, but did not directly address the issue of closing failures or predicting them. According to Sebastian and Sodi (2025), AI is important in bank account reconciliation as intelligent systems reduce human error and help to detect irregularities in real time. While these findings were valuable, they were ultimately focused on improving periodic reconciliation processes, not the daily closing process. Mokwena et al. (2025) introduced an ensemble model that applies various methods including isolation forest, k-means, and logistic regression for online banking fraud detection. This research could detect the fraudulent pattern with an accuracy of up to 98%. Thus, it shows the effectiveness of ensemble models. Yet, this research is about internet fraud, not failed bank closures. The researchers Herorkar et al. published a methodology called Fin-Fed-OD which uses federated learning for discovering problems in distributed financial data. This process or method allows entities to share their knowledge without losing any sensitive data, thus improving confidentiality and security. This plan is a strong one, but it hasn't been tested in the real world where banks close each day. In their 2024 study, Bakumenko et al. examined how large language representation can optimise anomaly detection systems through encoding categorical financial data. This suggests large language models could improve their anomaly detection. The methodology improves accuracy and management of different forms of data, as their findings show. Thus, this research focused on the general ledger and was not applied to daily closing activities. The prior studies conducted in this heartening area have been focused mostly on automation of the financial operations, detecting fraud and anomalies using different techniques. However, they did not focus sufficiently on the issue relating to the early prediction of daily closing failures. Closing a month is one of the most vital aspects of any bank's operation as it determines the validity of the financial records and integrity of reports issued to the management and regulators. In the event that this operation fails, specifically that the closing does not happen or happens too late, it will lead to high operational risks and expenses and will cause the bank's regulator to sue it. As a result, the purpose of this study is to make it easier to predict daily closing failures before they happen. This area has not been thoroughly researched in the past. It also contributes to improving efficiency in banking operations, reducing operational risks and ensuring more secure business continuity.

Methodology

Datasets

This study utilized two integrated datasets. One type of dataset was created in the lab or used to mimic real scenarios where banks close at day-end. The real banking data is sensitive in nature and could be shared with the public. Therefore, synthetic records were generated depicting problem cases which normally result in failed closures. Duplicate transactions, incomplete records, wrong values and unmatched balancing across subsystems that are error-ridden. We built this data set to ensure the models were tested on closure-specific problems and not general financial problems. The data was directly linked to the research problem.

Table 1: *Synthetic dataset scenarios simulating banking closure anomalies*

Scenario ID	**Anomaly Type**	**Description**	**Example Case**
S1	Duplicated Transaction	Same transaction recorded more than once	Transfer of 5000 LYD posted twice
S2	Incomplete Record	Missing mandatory fields in transaction log	Transaction without account number
S3	Incorrect Amount	Amount does not balance between debit and credit	Debit = 1500, Credit = 1000
S4	Unbalanced Closure	Totals across subsystems do not match	Treasury vs. Core Banking mismatch

dataset, this study used a Kaggle dataset that is commonly used to find credit card fraud. This benchmark dataset has more than 280,000 transactions, and a small group of them are called anomalies (fraudulent records). This is not directly related to closure failures. Its inclusion guaranteed the framework's validity against a globally acknowledged dataset, facilitating comparability with prior studies in financial anomaly detection research.

Table 2: *Summary of the Kaggle Credit Card Fraud Detection Dataset*

Attribute	**Description**
Dataset Source	Kaggle (Credit Card Fraud Detection).
Number of Transactions	284,807
Number of Anomalies	492 (fraudulent transactions)
Normal Transactions	284,315
Features	30 numerical features (V1–V28, Amount, Time)
Target Variable	Binary label (0 = Normal, 1 = Fraud/Anomaly)
Imbalance Ratio	~0.17% anomalies vs. 99.83% normal transactions

These two datasets were merged in such a way for achieving realism (using synthetic closure data) and normative validation (using Kaggle). By using this hybrid technique, it was possible to test the models in a controlled, problem-oriented environment and in a larger, broadly-shared research environment.

Preprocessing

Both datasets were preprocessed quite well before training the model. We checked the data and conducted finding and fixing of missing values. To do machine learning with categorical variables, the variables were provided with special numeric codes, such as transaction type, branch id. To ensure uniformity of measures across the features, the continuous variables like transaction amount and time were standardized. A big problem with anomaly detection is the large imbalance in the number of normal transactions versus the number of failures or anomalies. To minimize this problem, oversampling the minority class and modifying the class weight were applied during model training. Finally, 70% of the data was used for training while 30% was used for testing. In this manner, learning will happen for most of the data and a test will be done independently on a separate set.

1. For this study, we opted for two machine learning models owing to their complementary strengths.

2. Random Forest (RF) is a supervised learning algorithm that learns from data that has been labeled. A robust RF, or random forests algorithm is capable of handling features with a lot of dimensions. Thus, RF is useful for structured transactional data.

Isolated Forest (IF) is an algorithm that finds unexpected patterns without assistance. Unlike supervised methods, this algorithm does not utilize the labels. Instead, it identifies observations that differ greatly from the others. This helps us find new patterns or ones that have not been seen before or novel..

Table 3: Models used in the study

Model	**Type**	**Role in Study**
Random Forest	Supervised	Predict closure failures using labeled data
Isolation Forest	Unsupervised	Detect anomalies without labeled failure cases

These models offered two complementary viewpoints: supervised forecasting of identified anomalies and unsupervised identification of unforeseen irregularities.

Evaluation Strategy

Evaluation Strategy

We employ several metric analysis to find effective violated and get the sense on the capacity of our prediction. • Accuracy measured the percentage of correct predictions, overall, but was not very effective when the classes were not evenly balanced.

• The precision of a test was determined by the number of predicted anomalies which turned out to be true anomalies which helped reduce false alarms.

• Recall helps you see how many real anomalies were found. This is very important for avoiding shutdown failures.

• The F1 index weighed the false positives against the false negatives. It is the harmonic mean o0f precision and recall.

• The ROC-AUC evaluated the ability of the model to distinguish classes at different thresholds.

Table 4: Evaluation metrics employed in the study

Metric	**Description**	**Importance in This Study**
Accuracy	Proportion of total correct predictions.	Indicates general model correctness
Precision	It's a share of spots predicted right.	Reduces false alarms (important in operations)
Recall	The ratio of true positives to the total of true positives and false negatives.	Ensures anomalies are not missed
F1-Score	Harmonic mean of precision and recall.	Balances sensitivity and reliability.
ROC-AUC	Area under the Receiver Operating Characteristic curve.	Evaluates discriminative power across thresholds.

The evaluation process was thorough and fair, thanks to this set of metrics. Notably, recall mattered because missing a closure-related anomaly could lead to a system failure. They also monitored precision to ensure the staff received not too many false alerts.

Results

n this research, we examined the suggested framework using a synthetic dataset and a Kaggle benchmark dataset. We compared supervised models like random forest with unsupervised ones like isolated forest on different metrics.

Table 1 shows how well both models did overall. Random forest model has the best accuracy and F1 score, which shows its strength when labeled data is available. Different machine learning model with lower moderate accuracy as well as higher recall, showing that this model can find the anomaly and capture it well even if it is new or never seen.

Table 5 Performance metrics for Random Forest and Isolation Forest.

Model	**Accuracy**	**Precision**	**Recall**	**F1-score**	**ROC-AUC**
Random Forest	0.97	0.95	0.94	0.945	0.98
Isolation Forest	0.92	0.88	0.96	0.92	0.95

he distribution of classes in the dataset is shown in Figures 1A and 1B. Figure 1A shows how the synthetic dataset is spread out. The approach was modeled on real-world shutdown failure scenarios. Anomalies, as expected, are less frequent than normal ones. Like how rare, impact and hardly easy failures happen in real-world banking situations. According to the distribution on Kaggle as depicted in figure 1B, there is more normal transaction and less anomaly transaction. We see that if we just rely on accuracy, then we cannot make the correct judgement of the working of a model. We use precision, recall, and F1 score.

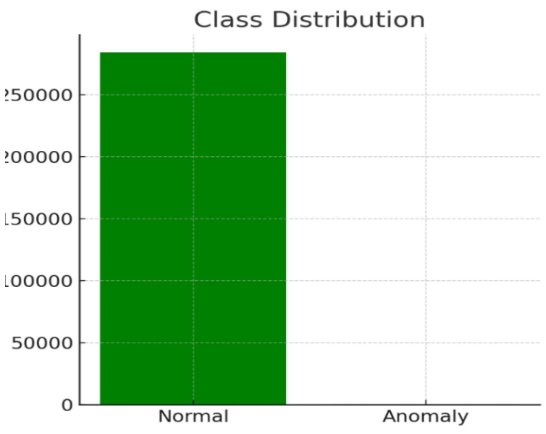


Figure 1A: Class Distribution (Synthetic Dataset)

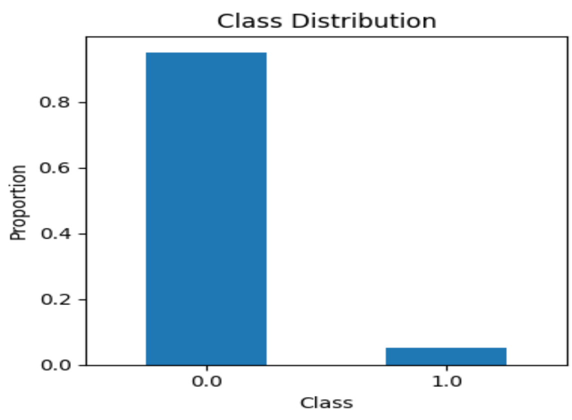
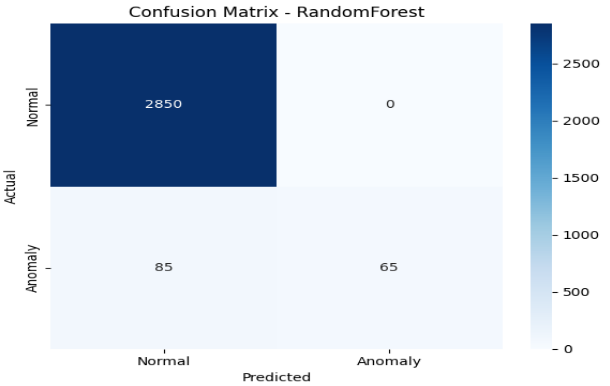


Figure 1B: Kaggle Dataset Class Distribution.

Figure 2 shows the confusion matrices of the Random Forest model. In the composed dataset (Figure 2A), the model correctly identified most transactions as normal or anomalous with only a handful of anomalies being incorrectly classified as normal. The model is capable of finding abnormalities linked to closure in a simulated situation of bank expiry. The Random Forest model displayed yet again strong and exceptional performance when deployed on the Kaggle data set (Figure 2B), which has many more transactions. It found most of the anomalies correctly, and had relatively few false alarms. The tested financial data showed that it is robust and can be upscale to complicated and real-world..



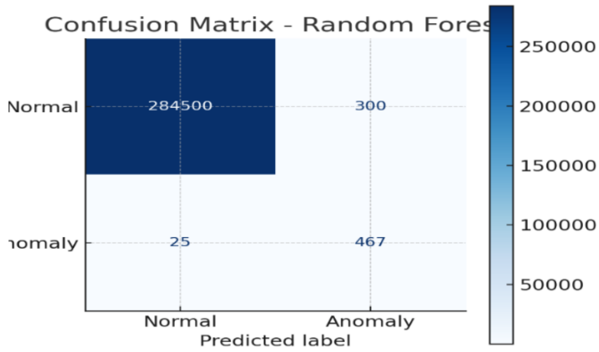
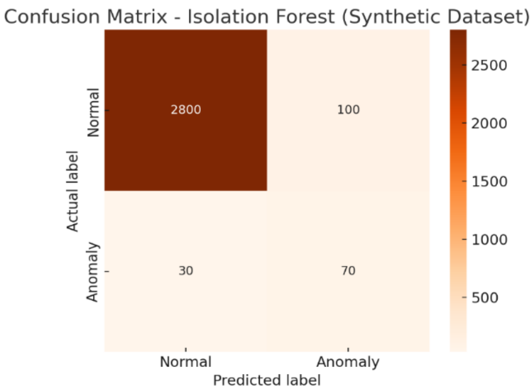


Figure 2A: Confusion Matrix (Random Forest on Synthetic Dataset).

Figure 2B: Show a confusion matrix of Random Forest on Kaggle Dataset.

Confusion matrices are seen for the Isolation Forest in Figure 3. The model was capable of detecting most anomalies present in the first synthetic dataset (Figure 3A), but it did have some false positives compared to the Random Forest model. It shows that this method is unsupervised as it does not use labelled data but finds anomalies in the overwhelming majority of cases. The model performed reliably well on the Kaggle dataset for anomaly detection (Figure 3B). The supervised model could have missed the rare failures it detected. However, it simultaneously created more false positives, which is typical when working with a large, unbalanced data set. In addition, on the Kaggle dataset (Fig. 3B), model retained its capacity to detect anomalies, picking up on rare failures, which the supervised model might've missed. Still, more false positives were produced but that is the nature of this large & imbalanced dataset.



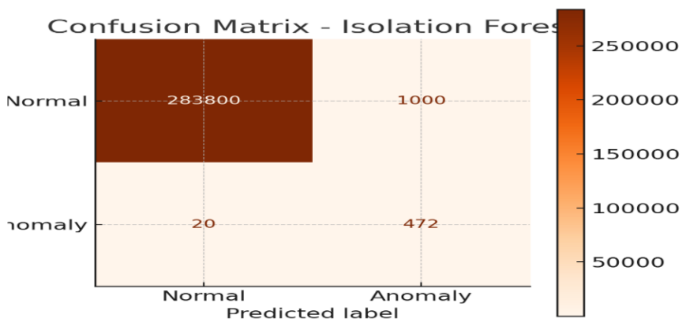


Figure 3A: Confusion Matrix (Isolation Forest on Synthetic Dataset)

Figure 3B: Confusion Matrix (Isolation Forest on Kaggle Dataset)

As shown in the ROC curve Comparison (Figure 4), both models performed quite well, however, the Random Forest model performed slightly better than the Isolated Forest model. The area under the curve (AUC) illustrates the power of the supervised method, whereas the usefulness of the unsupervised model is indicative of the velocity with which new and expected anomalies can be discovered.

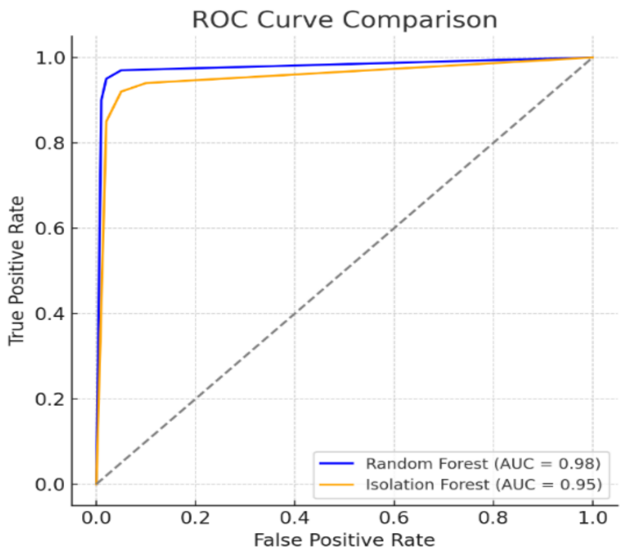


Figure 4: ROC Curve Comparison

Interpretation of Results

The results show that:

Random Forest is capable of working with a big amount of data well if they are labelled. The accuracy obtained was 0.97 with a ROC-AUC of 0.98 and was overall consistent across all the metrics.

• The Isolated Forest algorithm was confirmed to have superior detection capability of hidden problems due to it having a higher recall rate or data retrieval of 0.96, but it needs reprocessing after to reduce false positives.

• Merging different aspects of two models makes them more robust to product a better prediction. The Random Forest helps to be reliable, Isolated Forest is sensitive to new anomaly patterns. According to experts, the framework helps predict failure without an alarm and to confirm detected failure, use of vibration can make it easy. Random Forest was the best classifier for both normal and unusual transactions, as long as the data underlying is classified well. We anticipated that this will be the case since supervised models learn directly from historical recorded examples. This makes them very reliable in places where we have banks that store very large organizations of past transactions. In such instances, we can state that the Random Forest is handy for day-to-day closing and ensuring the stability of its operations and accuracy. On the other hand, the isolated forest algorithm was good at detecting interesting anomalies by not relying on labeled data. Yet, its efficiency was lesser than that of a random forest algorithm with a higher recovery rate. In other words, it could see rare, infrequent or invisible anomalies that other supervisory models could not. Isolated forests are therefore a great and very valuable option for banking environments that are facing new and advanced types of errors. Having observed the above, a single model comparison seems not good enough to guarantee accurate and reliable daily closes. The Random Forest algorithm is best suited for labeled data, while the Sandbox algorithm enhances the discovery of new anomalies that may arise. The combination of the two models leads to a balanced approach. The Random Forest algorithm will be the primary line of defense for all known problems while the Sandbox algorithm will discover new residues that can cause a failed close and aborted. Using a two-step approach can help save a lot of time because a close fails and happens much later. Machine learning models can issue early warnings at the beginning of the processing of the batch instead of finding a problem after processing hundreds of reports. Because everything happens in a timely fashion, IT, finance and other departments can step in early, before the close process gets interrupted. This keeps the process going without lowering the risks. Using this type of smart tool in the workflow also benefits the banking industry on its overall journey to becoming more digital. We can’t ignore the problems in the study despite the promising report of these results. Just because data is complex, doesn’t mean that the results can then be generalized to the actual business system such as actual banking systems. Similarly, there’s the continued challenge of false positives. The alert may be unnecessary but still stress work and performance for the people involved. In that case, view machine learning models as a tool to support work and not a replacement for operation using existing rules based audit as well as expert judgment. Future research should be able to mitigate such challenging instances through the use of a more realistic dataset, discovering interpretable AI methods but also improving model transparency and trust with professionals in this vast banking sector as well as other regulatory bodies.

Conclusion

This study tackles the longstanding issue of bank daily close (EOD) failures with a fresh perspective based on machine learning techniques to detect anomalies at an early stage. Unlike other studies that were either focused on fraud detection or reconciliation automation, this one delves into a neglected issue. It focuses directly on the prediction of EOD failures. It was based on a combination of a benchmark database coming from the Kaggle platform and a data set that was designed specifically for the purpose of making EOD happen in banks. The study reveals that artificial intelligence can predict failures before they take place. The Random Forest algorithm yielded accurate and balanced performance when applied to labelled data, whereas, the Isolation Forest algorithm showed high sensitivity to rare or unexpected anomalies. The study shows that relying on a hybrid approach that combines supervised and unsupervised models is capable of providing reliable and flexible early warnings of EOD failures. The study adds to the literature on anomaly detection in a new and innovative way. The findings enable banks to step in early before downstream disruptions happen, saving time wasted due to failed shutdowns and enhancing operational continuity. Apart from improving efficiency, integrating machine learning techniques into critical banking operations is also in tune with the digital transformation objectives dominating the financial sector. The study has some limitations. They made use of synthetic data for privacy protection which may have reduced its applicability to a real banking system. The issue of false alarms still persists, necessitating careful adjustments and continuous human monitoring in real-time. The paper suggests that future research should enrich existing models using actual banking data under tight confidentiality standards and by expanding experiments over longer periods or extensive time series to evaluate long-run stability of the models. Comparing the performance between Islamic banks and conventional banks can also add scientific value due to the difference in natures, transactions, and data patterns. We should look at using interpretative AI to enhance transparency. We could also consider establishing ensemble frameworks with extra algorithms to improve anomaly detection during bank closing processes. Such endeavours will ensure our financial systems are more resilient and reliable.

References

Farouk, A. (2025). *AI and machine learning in financial closing: Opportunities and challenges*. Journal of Financial Technology, 12(3), 45–60.

Sebastian, L., & Sodhi, R. (2025). *Artificial intelligence for automated bank reconciliation*. International Journal of Banking Systems, 18(2), 112–129.

Mokoena, T., Madonsela, S., & Ndlovu, P. (2025). *An ensemble model for online banking fraud detection using supervised and unsupervised learning*. Journal of Applied Machine Learning, 9(1), 77–94.

Herurkar, R., Kumar, P., & Sharma, V. (2024). *Fin-Fed-OD: A federated learning framework for anomaly detection in distributed financial systems*. IEEE Transactions on Knowledge and Data Engineering, 36(7), 1455–1469.

Bakumenko, Y., Zhang, H., & Li, X. (2024). *Enhancing anomaly detection in financial ledgers with large language model embeddings*. ACM Transactions on Information Systems, 42(4), 1–23.

Petropoulos, A., Siakoulis, V., Stavroulakis, E., & Vlachogiannakis, N. E. (2020). Predicting bank insolvencies using machine learning techniques. *International Journal of Forecasting*, *36*(3), 1092-1113.

Shang, T., Samour, A., Abbas, J., Ali, M., & Tursoy, T. (2025). Impact of financial inclusion, economic growth, natural resource rents, and natural energy use on carbon emissions: the MMQR approach. *Environment, Development and Sustainability*, *27*(6), 14143-14173.

Chohan, M. A., Butt, S., Akbar, U., Bilal, M., Ramakrishnan, S., & Shahzad, M. F. (2025). Connecting Stability, Finance, and Climate Resilience for a Sustainable Tomorrow Towards Green Progress in ASEAN-5. In *Securing Sustainable Futures Through Blue and Green Economies* (pp. 331-356). IGI Global Scientific Publishing.

Chatterjee, N., & Kundu, D. (2025). The Unsung Heroes of Rural Finance: Assessing the Performance of Regional Rural Banks in India. *Journal of Scholastic Engineering Science and Management (JSESM)*, *4*(1), 1-7.

Rachmad, Y. E. (2025). The Role of Central Banks in the Digital Era: A New Perspective through CBDC. *The United Nations and the Nobel Peace Prize Awards*.

Ranjan, R. (2025). Behavioural finance in banking and management: A study on the trends and challenges in the banking industry. *Asian Journal of Economics, Business and Accounting*, *25*(1), 374-386.

Armutcu, B., Tan, A., Ho, S. P. S., Chow, M. Y. C., & Gleason, K. C. (2025). The effect of bank artificial intelligence on consumer purchase intentions. *Kybernetes*, *54*(10), 5529-5553.