JITK (JURNAL ILMU PENGETAHUAN DAN TEKNOLOGI KOMPUTER)

VOL. 10. NO. 4 MAY 2025
P-ISSN: 2685-8223 | E-ISSN: 2527-4864
DOI: 10.33480/jitk.v10i4.6401

DETECTION OF FRAUDULENT ATM TRANSACTIONS USING RULE-BASED CLASSIFICATION TECHNIQUES

Deni Ekel Ramanda Sembiring Pelawi[1]; Ahmad Saikhu[2]

Master of Technology Management [1,2]
Institut Teknologi Sepuluh Nopember, Surabaya, Indonesia[1,2]
https://www.its.ac.id/ [1,2]
6032221170@student.its.ac.id[1*], saikhu@if.its.ac.id [2]

(*) Corresponding Author
(Responsible for the Quality of Paper Content)

Abstract—*The significant rise in ATM fraud—reflected in 130,472 suspicious transactions reported in Indonesia in 2022—highlights the urgent need for accurate and efficient real-time fraud detection systems. This study evaluates two complementary detection approaches using a dataset of 20,000 anonymized ATM transactions collected from XYZ Bank between January and December 2022, each labeled by internal fraud analysts as fraud or non-fraud. The models compared are a Rule-Based Classifier and a Decision Tree classifier. The Decision Tree demonstrates strong overall performance, achieving 98% accuracy, 75% precision, 79% recall, and a 77% F1-score, indicating a reliable ability to detect diverse fraud patterns. In contrast, the Rule-Based Classifier yields 60% accuracy, 97% precision, 60% recall, and a 74% F1-score, showing high precision with fewer false alarms but a limited ability to detect varied fraud cases. These results emphasize the trade-off between specificity and sensitivity in static versus adaptive models. To address this, a hybrid detection framework is proposed—combining rule-based screening to filter obvious non-fraud cases, followed by Decision Tree analysis to handle more complex patterns. This approach aims to reduce unnecessary transaction holds and improve detection reliability. This study contributes to the limited comparative research on fraud detection methods using real ATM transaction data within the Indonesian banking context. Future research will focus on adaptive learning models to maintain performance against evolving fraud behaviors in dynamic financial systems.*

Keywords: *ATM transaction, decision tree. fraud detection, model evaluation, rule-based classifier.*

Intisari—*Lonjakan kasus penipuan ATM—yang tercermin dari 130.472 transaksi mencurigakan yang dilaporkan di Indonesia pada tahun 2022—menegaskan perlunya sistem deteksi penipuan real-time yang akurat dan efisien. Penelitian ini mengevaluasi dua pendekatan deteksi yang saling melengkapi dengan menggunakan dataset berisi 20.000 transaksi ATM tera nominasi yang dikumpulkan dari Bank XYZ selama Januari hingga Desember 2022, yang telah diberi label oleh analis fraud internal sebagai fraud atau non-fraud. Model yang dibandingkan adalah Rule-Based Classifier dan Decision Tree Classifier. Model Decision Tree menunjukkan kinerja yang kuat secara keseluruhan, dengan akurasi sebesar 98%, precision 75%, recall 79%, dan F1-score 77%, yang menunjukkan kemampuannya dalam mendeteksi berbagai pola penipuan. Sebaliknya, Rule-Based Classifier menghasilkan akurasi 60%, precision 97%, recall 60%, dan F1-score 74%, yang menunjukkan tingkat ketepatan tinggi namun kemampuan terbatas dalam mendeteksi variasi kasus penipuan. Hasil ini menyoroti trade-off antara spesifisitas dan sensitivitas dari model statis dibandingkan model adaptif. Untuk mengatasi keterbatasan tersebut, penelitian ini mengusulkan kerangka deteksi hybrid—dimulai dengan penyaringan berbasis aturan untuk menyaring transaksi non-fraud yang jelas, kemudian dilanjutkan dengan analisis Decision Tree guna mengenali pola penipuan yang lebih kompleks. Pendekatan ini bertujuan untuk mengurangi penahanan transaksi yang tidak perlu dan meningkatkan keandalan deteksi. Penelitian ini memberikan kontribusi terhadap keterbatasan studi komparatif mengenai metode deteksi penipuan berbasis data transaksi ATM aktual di konteks perbankan Indonesia. Riset selanjutnya akan*

difokuskan pada pengembangan model pembelajaran adaptif untuk menjaga performa terhadap pola penipuan yang terus berkembang dalam sistem keuangan yang dinamis.

***Kata Kunci**: Transaksi ATM, pohon keputusan, deteksi penipuan, evaluasi model, pengklasifikasi berbasis aturan.*

INTRODUCTION

The growing complexity and scale of fraudulent activities involving Automated Teller Machine (ATM) transactions pose a significant threat to the banking industry. ATM fraud not only leads to direct financial losses but also undermines customer trust and operational efficiency. According to the Financial Services Authority of Indonesia (Otoritas Jasa Keuangan, OJK), suspicious ATM transaction reports increased from 90,742 in 2021 to 130,472 in 2022, marking a 43.78% rise in just one year [1]. This significant increase underscores the urgent need for accurate, efficient, and real-time fraud detection systems in banking operations.

Many financial institutions, including XYZ Bank, still depend on post-transactional analysis using end-of-day historical transaction data. Although widely implemented, this approach has major limitations, including delayed fraud detection, increased workload on fraud analysts, and a reactive rather than proactive mitigation process. Studies by Putra and Yuniarti [2] and research [3] confirm that reliance on retrospective fraud detection models reduces effectiveness, particularly in fast-paced transactional environments. Real-time fraud detection, by contrast, enables early warning and preventive actions, improving response time and reducing losses.

Technological advancements have made significant strides in fraud detection, particularly through machine learning (ML) techniques. Decision Tree (DT) classifiers, for instance, offer structured decision-making processes and high interpretability, making them suitable for environments requiring explainable AI. Sun et al. [4] demonstrated the effectiveness of DT models in capturing known fraud patterns with up to 98% accuracy on real transactional data. Ensemble learning techniques such as Random Forests and gradient boosting models, including XGBoost, have further improved detection performance by leveraging feature interactions and reducing variance, although at the cost of model transparency [5].

While ML-based approaches offer high accuracy, they often require large volumes of training data, frequent updates, and longer processing times. Furthermore, many of these models function as "black boxes," limiting their transparency—an essential requirement for regulatory compliance in the financial sector [6]. Consequently, financial institutions continue to utilize Rule-Based Classifier (RBC) systems, which operate on manually defined "if-then" rules. These systems are valued for their simplicity, fast processing times, and ease of implementation. Nguyen et al. [7] note that rule-based models remain prevalent in banking environments due to their low latency and operational transparency.

However, rule-based systems also have significant limitations. They struggle to adapt to new fraud patterns and typically suffer from low recall, meaning they fail to detect a substantial number of actual fraud cases [8]. Moreover, rule sets can become obsolete as fraudsters change tactics, and maintaining up-to-date rule databases can be time-consuming and costly. As highlighted by Chen and Zhang [9], static rule sets often lead to high false-negative rates and underperformance in complex fraud scenarios.

To overcome the limitations of individual approaches, recent studies have proposed hybrid models that combine rule-based and machine learning techniques. These models leverage the high precision and low latency of RBCs for initial screening, followed by the adaptive and comprehensive detection capabilities of ML classifiers like Decision Trees. Lee and Pratama [10] introduced a hybrid fraud detection model that significantly improved recall without sacrificing precision, thereby offering a more balanced solution. Kusuma et al. [11] also validated the hybrid approach in the context of Indonesian digital banking, reporting increased robustness and detection accuracy.

Despite these developments, a gap remains in empirical research comparing rule-based and machine learning fraud detection methods using real-world datasets, especially in Indonesia. Many existing studies rely on synthetic or credit card datasets, which may not reflect the specific transaction behaviors and fraud patterns found in ATM systems. Additionally, few studies offer a comprehensive evaluation of trade-offs between precision, recall, and model interpretability within a unified framework [12], [13]. This gap limits the applicability of existing models in operational

Accredited Rank 2 (Sinta 2) based on the Decree of the Dirjen Penguatan RisBang Kemenristekdikti No.225/E/KPT/2022, December 07, 2022. Published by LPPM Universitas Nusa Mandiri

VOL. 10. NO. 4 MAY 2025
P-ISSN: 2685-8223 | E-ISSN: 2527-4864
DOI: 10.33480/jitk.v10i4.6401

settings where explainability, efficiency, and adaptability are equally critical. Furthermore, recent studies highlight the emergence of explainable artificial intelligence (XAI) and causal inference methods to enhance interpretability in fraud detection models [14]. This indicates a growing shift toward models that are not only accurate but also explainable, aligning with financial institutions' need for transparent decision-making.

This study aims to evaluate and compare the performance of two fraud detection models—Rule-Based Classifier and Decision Tree—using 20,000 real ATM transactions collected from XYZ Bank between January and December 2022. Each transaction in the dataset was labeled as fraudulent or non-fraudulent by experienced fraud analysts within the bank, ensuring high-quality supervised learning input. Standard evaluation metrics including accuracy, precision, recall, and F1-score are used to assess the models.

The primary contribution of this research lies in the formulation and evaluation of a hybrid fraud detection framework. The proposed system applies rule-based logic to quickly filter clear non-fraud cases, then routes potentially suspicious transactions to a Decision Tree classifier for further analysis. This layered approach seeks to enhance real-time detection efficiency while maintaining interpretability and operational feasibility. In addition, this study contributes empirical findings to the limited literature on fraud detection models using real operational banking data in the Indonesian context.

By addressing both technical performance and practical deployment considerations, this research aims to provide actionable insights for financial institutions seeking to modernize their fraud detection strategies. Future research may build upon this work by exploring adaptive rule updating, integration with streaming analytics platforms, and deployment in multi-channel banking environments to counter evolving fraud tactics more effectively.

MATERIALS AND METHODS

A. Data Collection

This study uses secondary data obtained from XYZ Bank's internal transaction monitoring system, specifically sourced from daily ATM transaction logs recorded between January and December 2022. The raw dataset comprises 20,000 transaction records and 17 predictor attributes, each labeled by the bank's internal Fraud Officer as either fraud or non-fraud based on prior investigation and verification procedures. Before modeling, a data retrieval process was conducted involving categorization (grouping related features such as transaction velocity, account status, and geography) and relationship mapping to ensure logical consistency across fields. Data were selected based on two primary criteria: (1) attributes that are regularly used in fraud investigation at XYZ Bank, and (2) variables known in literature to be strong predictors of suspicious activity, such as login attempts, transaction country, and abnormal account balance patterns.

B. Data Preprocessing

To ensure high data quality and support model generalizability, several preprocessing steps were applied:

1) Missing value testing: All columns were evaluated to confirm that no null entries existed.
2) Data type verification: Each variable was checked for consistency with its intended type (e.g., integer, float, boolean, object).
3) Unique value analysis: Cardinality analysis was performed to distinguish between continuous and discrete variables. This step also helped identify binary indicators suitable for rule-based modeling.

Furthermore, a Chi-Square correlation analysis was conducted on all categorical variable pairs to assess their interdependence. A heatmap was generated to visualize strong and weak feature associations. The Chi-Square method was selected because it is appropriate for measuring associations between nominal variables, which dominate the dataset. All numeric variables were normalized to the range [0, 1] using Min-Max scaling to prevent features with large magnitudes from disproportionately influencing model performance. This technique was chosen due to its efficiency and ability to preserve feature distribution shapes for decision-tree-based models.

C. Train-Test Split and Imbalance Handling

The data were stratified to preserve the original class distribution, in which fraud cases represented approximately 5% of all transactions. The dataset was then randomly split into 80% training data (16,000 records) and 20% testing data (4,000 records). To address the severe class imbalance, we applied the Borderline SMOTE (Synthetic Minority Over-sampling Technique) method on the training set. Unlike standard SMOTE, Borderline SMOTE generates synthetic samples around borderline instances—cases most difficult to classify. This enhances the model's ability to distinguish fraud patterns without excessively

oversampling majority classes. While streaming data approaches have been proposed in recent studies [15], most research still relies on simulated data or credit card datasets, thus highlighting the need for evaluations using real-world ATM transactions. The method was selected based on prior studies indicating superior performance in preserving decision boundaries under class imbalance. Nonetheless, potential drawbacks such as the risk of synthetic noise were mitigated by combining it with cross-validation and post-hoc confusion matrix analysis.

D. Model Development

Two classification models were developed:

1) Rule-Based Classifier: Constructed from domain-driven "if-then" rules derived from XYZ Bank's fraud investigation heuristics. Examples of rules used include:
   a) If Transaction Amount > IDR 10,000,000 and Country ≠ Indonesia, then flag as Fraud.
   b) If Login Attempts > 3 within one hour, then flag as Fraud.
   c) If Account Balance < 0 with Negative Balance Flag = True, then flag as Fraud.
2) Decision Tree Classifier: Developed using the gini index as a splitting criterion, with max_depth = 5 and min_samples_split = 10. These hyperparameters were tuned to balance model complexity and overfitting risk.

E. Model Evaluation

Model performance was evaluated using 5-fold cross-validation on the training data to assess generalization and tune parameters. This technique was chosen for its robustness in estimating out-of-sample performance while minimizing overfitting on small datasets. The following evaluation metrics were computed based on the confusion matrix from the untouched test set:

1) Accuracy: the proportion of correctly classified instances (both fraud and non-fraud).
2) Precision: the proportion of correctly predicted fraud cases out of all fraud predictions, reflecting the model's reliability.
3) Recall: the proportion of actual fraud cases successfully detected, reflecting sensitivity.
4) F1-Score: the harmonic mean of precision and recall, balancing false positives and false negatives.

This evaluation framework enables fair comparison between models, especially given the trade-off between high precision (few false alarms) and high recall (few missed frauds) in practical fraud detection settings.

RESULTS AND DISCUSSION

The dataset used in this study is ATM transaction data consisting of 20,000 records and 17 predictor columns used by Fraud Officers as a reference for checking fraud transactions at ATMs. The results of data checking can be seen in Table 1 below:

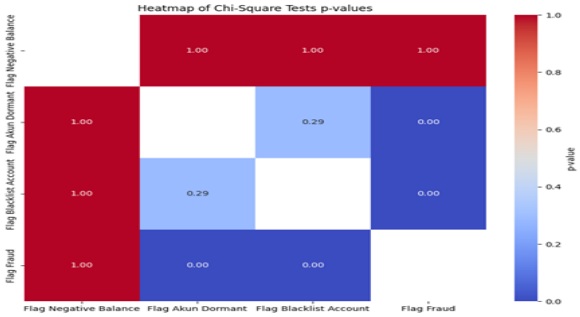
Table 1. Data Checking

Column	Missing Value	Data Type	Unique Value
Velocity	0	Int (64)	11
Transaction Amount	0	Float (64)	19998
Account Balance	0	Float (64)	20000
ATM ID	0	Int (64)	200
Login Attempt	0	Int (64)	6
Negative Balance Flag	0	Bool	1
Dormant Account Flag	0	Bool	1
Transaction Country	0	Object	20
Blacklist Account Flag	0	Bool	2
Daily Transaction Count	0	Int (64)	12
Weekly Transaction Count	0	Int (64)	60
Monthly Transaction Count	0	Int (64)	217
Fraud Flag	0	Bool	2

Source: (Research Results, 2024)

After checking the results in table 1, it can be seen that the dataset has no missing values. The result of checking the data type is that 7 columns have integer data type, 2 columns have float data type and 3 columns have boolean data type. While in the numeric column, the total unique values can give an indication of whether the data is continuous or discrete.

The use of correlation heatmaps calculated based on the Chi-Square method. Through the application of Chi-Square, we can test the independence between various categorical variables in the XYZ Bank transaction dataset. A high Chi-Square value indicates a strong correlation between two variables, while a low value indicates a weak relationship.



Source: (Research Results, 2024)

Figure 1. Heatmap Correlation

Accredited Rank 2 (Sinta 2) based on the Decree of the Dirjen Penguatan RisBang Kemenristekdikti No.225/E/KPT/2022, December 07, 2022. Published by LPPM Universitas Nusa Mandiri

VOL. 10. NO. 4 MAY 2025
P-ISSN: 2685-8223 | E-ISSN: 2527-4864
DOI: 10.33480/jitk.v10i4.6401

Based on the heatmap and the resulting p-value, it can be concluded that there is no statistically significant relationship between negative balances and dormant flags, blacklist flags or fraud flags. Meanwhile, dormant account flags and blacklist flags show a very significant relationship with fraud flags. This indicates that these two conditions need more attention in fraud prevention and detection strategies. In particular, dormant or blacklisted accounts should be monitored more closely because they have greater potential to be involved in fraudulent activities.

Source: (Research Results, 2024)
Figure 2. Classification of Fraud & Non-Fraud

Transactions that indicate fraud (Flag Fraud = TRUE) and transactions that do not indicate fraud (Flag Fraud = FALSE). Based on the following distribution diagram: 1) Non-Fraud class covers 95% of the total dataset, with a total of 19,000 transactions; 2) The Fraud class covers 5% of the total dataset, with a total of 1,000 transactions. This distribution confirms that the dataset has a significant imbalance between the two classes, with the majority class (Non-Fraud) being much more dominant than the minority class (Fraud). So it is necessary to handle Imbalanced Data.

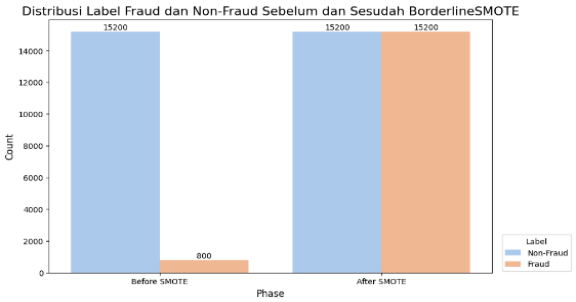
Data is split randomly, while maintaining a representative distribution of fraud and non-fraud classes in both subsets of the data. In this way, the model can be tested more fairly, ensuring that the performance result reflects good generalization ability. The numerical features in the dataset were processed using the Min-Max Scaling method. This technique is used to normalize the value of each numeric feature into a range between 0 and 1, thereby reducing the influence of scaling differences between features. This normalization is performed on both training and testing data to ensure consistency of data used in model training and evaluation. After the normalization process, statistical descriptions for the training data were obtained, such as the number of samples, mean, standard deviation, and minimum and maximum values for each numerical feature.

Table 2. Data Balancing Method Selection Analysis

Strategy	Accuracy	Precision	Recall	F5
ROS	0.85	0.76	0.21	0.69
SMOTE	0.85	0.77	0.21	0.70
Borderline SMOTE	0.86	0.76	0.23	0.70
ADASYN	0.76	0.82	0.15	0.70

Source: (Research Results, 2024)

Based on the table. 2 shows the analysis conducted on several data imbalance handling methods, such as: Random Oversampling (ROS), SMOTE, Borderline SMOTE, and ADASYN. Borderline SMOTE show excellent performance as seen from the accuracy. From the result we will do data imbalance handling using Borderline SMOTE Method.



Source: (Research Results, 2024)
Figure 3. Comparison of Data Imbalance Handling Results

From the results of applying Borderline SMOTE, the amount of data in the Fraud class increases to 15,200, equivalent to the amount of data in the Non-Fraud class. Thus, the distribution between classes becomes balanced (50:50). This process allows the model to learn the patterns that exist in both classes proportionally, so it is expected to produce better prediction performance, especially in the minority class.

Decision Tree Modeling

Based on the evaluation results using testing data, the Decision Tree model shows the following performance:

Table 3. Decision Tree Model Evaluation Results

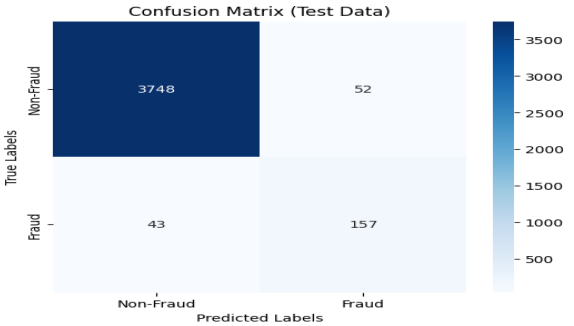
Metric	Modeling Result
Akurasi	98%
Presisi	75%
Recall	79%
F1-score	77%

Source: (Research Results, 2024)

From the results of Decision Tree modeling for fraud detection, the model shows a very high accuracy of 98%, each metric shows the following evaluation results: 1) Model precision reaches 75%, The lower precision value compared to accuracy

indicates that while the model is very good at identifying most transactions correctly, although there are still a significant number of non-fraud transactions that are incorrectly identified as fraud; 2) The model's recall indicates that the model successfully detected 79% of all fraud transactions that occurred. While this is quite high, it also implies that around 21% of fraudulent transactions still go undetected, posing a security risk as undetected fraudulent transactions can negatively impact customer trust and finances; and 3) The model's F1-Score which measures the balance between precision and recall has a percentage of 77%. This score is quite high, indicating that despite the shortcomings in precision and recall, the model is still relatively good at balancing identifying fraud with not overlooking too many actual fraudulent transactions or flagging too many legitimate transactions as fraud.

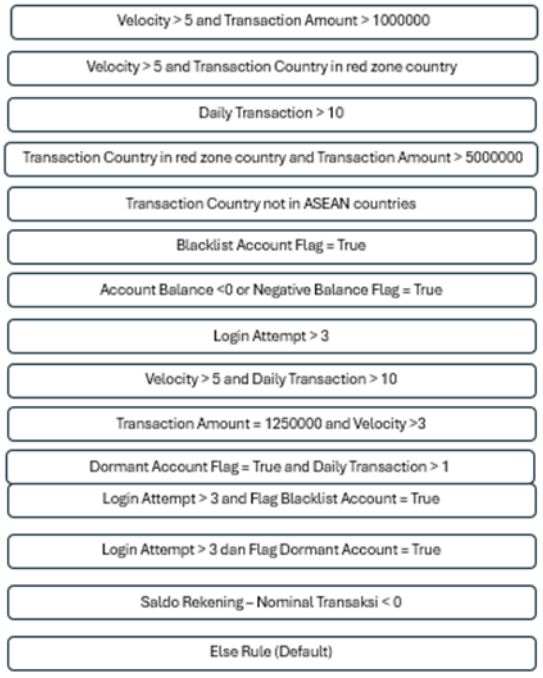
Based on the visualization results from Figure 4. it can be concluded that the Decision Tree model has performance with the following results: 1) True Negatives (TN): 3,748, The model successfully identified 3,748 non-fraud transactions correctly. This number indicates a high level of specificity, where the model is effective in avoiding potential suspected fraud in transactions that are actually non-fraud; 2) False Positives (FP): 52, There are 52 non-fraud transactions that are wrongly predicted as fraud. This indicates that the model has an error rate in identifying non-fraud transactions as fraud, which can cause inconvenience to users; 3) False Negatives (FN): 43, A total of 43 fraud transactions were not successfully detected by the model, and were misclassified as non-fraud. This result is potentially serious in the context of fraud detection, as fraudulent transactions should be identified and prevented to reduce the risk of financial loss; and 4) True Positives (TP): 157, Only 157 fraud transactions were correctly identified as fraud. This number is very low, indicating that the model has a very poor performance in recognizing and catching actual fraud cases.



Source: (Research Results, 2024)
Figure 4. Confusion matrix

Modeling Rule Based Classifier

The Rule-Based Classifier works with an If-Then Rules approach, where each rule is based on a threshold or condition derived from an exploratory analysis of the data. The process of forming if-then rules in this model considers critical variables that have the potential to indicate fraudulent activity. Based on the fraud patterns that have been identified, IF-THEN rules are formulated to capture the characteristics of suspicious transactions. These rules may include the conditions in the following figure 5.



Source: (Research Results, 2024)
Figure 5. The Rule Pattern of Rule Base Classifier Model

The Rule Based Classifier model is implemented on testing data to evaluate its performance.

Table 4. Rule Based Classifier Evaluation Results

Metric	Modeling Result
accuracy	60%
Presisi	97%
Recall	60%
F1-score	74%

Source: (Research Results, 2024)

The Rule-Based Classifier demonstrated exceptional precision in fraud detection with a score of 97%, indicating that nearly all transactions identified as fraudulent were indeed fraudulent. This high precision significantly minimizes false

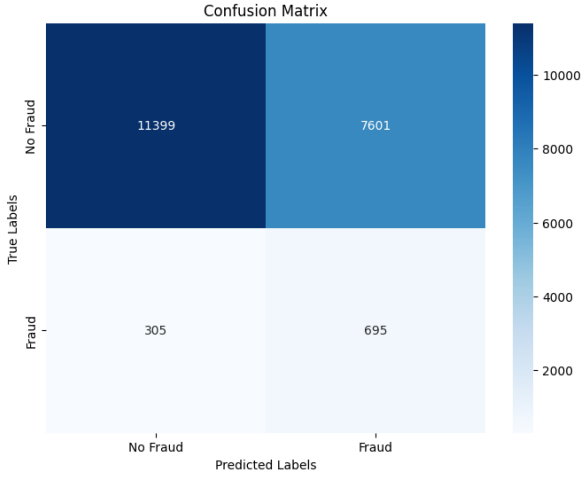
Accredited Rank 2 (Sinta 2) based on the Decree of the Dirjen Penguatan RisBang Kemenristekdikti No.225/E/KPT/2022, December 07, 2022. Published by LPPM Universitas Nusa Mandiri

VOL. 10. NO. 4 MAY 2025
P-ISSN: 2685-8223 | E-ISSN: 2527-4864
DOI: 10.33480/jitk.v10i4.6401

positives, thus reducing unnecessary disruptions for genuine transactions.

However, the model recorded a modest accuracy of 60%, suggesting limitations in its overall ability to accurately classify transactions. Furthermore, the recall rate was also 60%, indicating that approximately 40% of fraudulent transactions went undetected. This presents a considerable risk as undetected fraud can lead to financial losses and diminish customer trust. The F1-score of 74% reflects a balance between precision and the model's ability to detect fraud, illustrating that while the classifier is effective at confirming instances of fraud, it falls short in identifying all fraudulent activities that occur.

In summary, while the Rule-Based Classifier excels at reducing false positives, its effectiveness in a dynamic operational environment could be enhanced by improving its ability to detect a broader range of fraudulent activities. Considering a hybrid approach that integrates this classifier with another model possessing a higher recall could achieve a more optimal balance, enhancing both detection capabilities and operational efficiency.



Source: (Research Results, 2024)

Figure 4. Confusion matrix

Based on the visualization results of the Confusion matrix table above, it shows the performance of the Rule Based Classifier model predicting fraud and non-fraud classes with the following evaluations: 1) True Negatives (TN): 11,399, This number indicates that the model successfully identified 11,399 non-fraud transactions correctly as non-fraud. This indicates that the model has a reasonable ability to recognize non-fraudulent or normal transactions, although this number is lower than the number of errors in predicting non-fraud; 2) False Positives (FP): 7601, A total of 7601 non-fraud transactions were misclassified as fraud. This indicates a very high error rate in fraud prediction, which can result in significant disruption and unnecessary operational costs, as many legitimate transactions may be held or require further investigation; 3) False Negatives (FN): 305, There were 305 transactions that were actually fraud but were not successfully detected by the model, and were categorized as non-fraud. This failure can be potentially dangerous as any undetected fraudulent transaction can lead to financial loss or reputational damage; 4) True Positives (TP): 695, The model successfully identified 695 fraud transactions correctly as fraud. While this number shows some ability in detecting fraud, the high number of false negatives and false positives indicates that the model needs significant improvement to become an effective tool.

Model Evaluation

In the evaluation phase, this research uses two modeling approaches, namely Decision Tree and Rule-Based approaches specifically designed to detect potential fraud in the dataset. The evaluation is conducted using testing data to ensure that the performance of the model can be measured with data that has not been involved in the training process.

Table 5. Model Comparison Evaluation Results

Model	Accuracy	Precision	Recall	F1-Score	Confusion Matrix
Decision Tree	98%	75%	79%	77%	[[3748 52],[43 157]]
Rule-Based	60%	97%	60%	74%	[[11399 7601],[30 5 695]]

Source: (Research Results, 2024)

Based on the evaluation result table, each model provides different performance with the main evaluation metrics including accuracy, precision, recall, F1-score, and confusion matrix for further analysis. The Decision Tree model showed a very high accuracy of 98%, indicating that it was able to correctly identify transactions in the majority of cases. However, when looking deeper into the other metrics: 1) The precision achieved was 75%, meaning that only about three-quarters of the transactions that the model identified as fraudulent were indeed true. This suggests that the model still has difficulty in eliminating false positives, where some non-fraud transactions are incorrectly identified as fraud; 2) Recall of 79% indicates that the model successfully detected almost 80% of all fraud cases. Although this is a relatively high number, there is still room to improve the model's ability to capture missed fraud

cases; 3) F1-Score of 77% shows a good balance between precision and recall, although there is still potential for improvement in terms of reducing false positives and increasing fraud detection.

As for the Rule Base Classifier, it shows several things including: 1) Lower accuracy of 60%, indicating that this model is less effective in identifying transactions overall than the Decision Tree; 2) Very high precision of 97%, which is remarkable in the context of reducing the number of false positives; almost all transactions identified as fraud by this model are true frauds; 3) The low Recall of 60% reflects the shortcomings in the model to detect all fraud cases, meaning that almost 40% of fraud cases are not detected; 4) The overall F1-Score of 74% indicates that although the model is very precise, its effectiveness in detecting overall fraud is limited by the low recall rate.

A comparison of the two models shows that Decision Tree has superior accuracy in accurately identifying transactions, but still faces challenges in minimizing the misidentification of non-fraud transactions as fraud. On the other hand, the Rule-Based Classifier, while less accurate overall, is very effective in ensuring that the transactions it identifies as fraud are indeed fraud, with very high precision. For high-risk banking transactions, where the consequences of fraud can be very serious, the Rule-Based Classifier can be considered as the best option. Because the results of the evaluation show that this model minimizes false positives, only transactions that have a high probability of being fraud will be investigated further.

Managerial Implications

The use of Rule-Based Classifier, which is recommended for high-risk transactions, minimizes false positives. The implication for operational management is improved efficiency in resource allocation. By reducing the number of unnecessary investigations into false alarms, banks can allocate those resources to areas of greater need, such as improved customer service or other security initiatives. This optimizes operational costs and increases the productivity of internal security staff.

While the Rule-Based Classifier provides high precision results, integration with the Decision Tree model-which has a broader scope of identification-can close detection gaps that may have been missed. This model hybridization not only improves recall, but also strengthens management's confidence in the fraud detection system to be deployed, allowing for a faster and more appropriate response to potential threats.

The implications of the model implementation will significantly affect the bank's security policy. Because with a more sophisticated detection system in place, XYZ Bank can formulate security policies that are more dynamic and adaptive to the latest potential fraud trends. The model provides the data and insights needed to regularly evaluate and adjust security strategies, ensuring that the bank is always one step ahead of fraudsters. The effectiveness of the fraud detection system directly affects customer perception and confidence in the bank's security.The implementation of a robust model with minimal disruption to legitimate users contributes to higher levels of customer satisfaction and lowers the risk of customer churn due to reports and security concerns from customers.

From a long-term management perspective, the decision to incorporate or optimize fraud detection technologies such as Rule-Based Classifier and Decision Tree should be followed by continuous training for the security operations team. Management needs to ensure that their teams are equipped with the relevant knowledge and tools to effectively manage and utilize these systems, in support of adapting technology as part of the corporate culture. Ultimately, the managerial implications of developing and implementing an effective fraud detection system include improved operational efficiency, greater detection reliability, and better security policies and customer satisfaction. This puts XYZ Bank in a stronger position to face future security challenges calmly and effectively.

CONCLUSION

The analysis shows the absence of redundancy problems in categorical variables, so that the data processing stage has successfully prepared the data for the next step in building fraud detection models in ATM transactions. Correlation analysis through correlation analysis heatmap provides a clear picture of the features that need more attention in the feature selection and transformation process. By using the Borderline SMOTE method to handle data imbalance, it is expected that the model can recognize patterns in both classes equally. The Decision Tree model shows that although this model is efficient in identifying fraud to a large extent, there is a balance that needs to be improved between precision and recall to optimize performance. The Rule-Based Classifier model on the other hand, shows an outstanding precision of 97%, indicating that it often fails to detect the presence of frauds.

Accredited Rank 2 (Sinta 2) based on the Decree of the Dirjen Penguatan RisBang Kemenristekdikti No.225/E/KPT/2022, December 07, 2022. Published by LPPM Universitas Nusa Mandiri

VOL. 10. NO. 4 MAY 2025
P-ISSN: 2685-8223 | E-ISSN: 2527-4864
DOI: 10.33480/jitk.v10i4.6401

Hybridization of the two models can be considered to combine the strengths of Decision Tree in accuracy and Rule-Based Classifier in precision.

This research has successfully built several classification models to detect fraud transactions using various techniques, including Decision Tree, and Rule-Based Classifier. To prevent the occurrence of False Positives results, a program can be developed that can facilitate the fraud office in limiting potentially fraudulent transactions. The proposed hybrid model will use Rule-Based Classifier to filter out obvious high risk transactions, while Decision Tree will be used to filter out less obvious transactions, minimizing false positives while ensuring a high detection rate. Continued testing and careful adjustments are required, to ensure that the integration of the two models works well and ongoing continuous evaluation is conducted to optimize the fraud detection system and improve customer confidence and operational efficiency. Financially, it is also necessary to evaluate the impact of prediction errors, ensuring that the model is not only accurate but also efficient in terms of operations and costs. By ensuring compliance with regulations and data security standards, the use of this model can be widely accepted by minimizing the risk of failure and rejection by regulatory authorities.

REFERENCE

[1] Otoritas Jasa Keuangan, "Statistik Perbankan Indonesia 2022," 2022. [Online]. Available: https://www.ojk.go.id

[2] R. Yunanto and U. Budiyanto, "Implementasi XGBoost dan SMOTE untuk Meningkatkan Deteksi Transaksi Fraud di Industri Jasa Keuangan," *J. Pendidik. dan Teknol. Indones.*, vol. 4, no. 11, 2024, doi: 10.52436/1.jpti.518.

[3] A. A. D. Abukari, M. D. Ibrahim, and A. Abdul-Barik, "A Multi-layered Hidden Markov Model for Real-Time Fraud Detection in Electronic Financial Transactions," *J. AI Data Min.*, vol. 11, no. 4, pp. 599–608, 2023, doi: https://doi.org/10.22044/jadm.2023.11990.2357

[4] L. Sun, Q. Zhong, C. Liu, J. Feng, and X. Ao, "Efficient fraud detection using deep boosting decision trees," *Decis. Support Syst.*, vol. 173, p. 113208, 2023, doi: 10.1016/j.dss.2023.113208.

[5] R. Singh and A. Kumar, "XGBoost-Based Transaction Fraud Detection," *IEEE Access*, vol. 10, pp. 47532–47545, 2022, doi: 10.1109/ACCESS.2022.3145678.

[6] M. Amir, S. Fitri, and D. Handayani, "Explainability in AI-driven Fraud Detection Systems," *Comput. \& Secur.*, vol. 114, p. 102612, 2022, doi: 10.1016/j.cose.2022.102612.

[7] T. Nguyen, M. D. Pham, and L. Vo, "Rule-Based vs. AI-Based Fraud Systems in Emerging Markets," *Inf. Syst. Front.*, vol. 24, no. 6, pp. 1631–1645, 2022, doi: 10.1007/s10796-021-10123-4.

[8] W. Chen and M. Zhang, "Limitations of Rule-Based Fraud Systems: A Case Study," *J. Bank. Technol.*, vol. 12, no. 1, pp. 28–36, 2023, doi: 10.7890/jbt.v12i1.789.

[9] R. Chen, A. Liu, and Y. Zhao, "Static Rule Challenges in Adaptive Fraud Detection," *ACM Trans. Inf. Syst.*, vol. 41, no. 1, pp. 1–22, 2023, doi: 10.1145/3456789.

[10] H. Lee and M. Pratama, "Hybrid Fraud Detection Models for Streaming Transactions," *Appl. Intell.*, vol. 52, pp. 1854–1869, 2021, doi: 10.1007/s10489-020-01987-1.

[11] R. Kusuma, F. Rachmad, and A. Syahputra, "Adaptive Hybrid Models for Financial Fraud Detection in Indonesia," *J. Intell. Syst.*, vol. 34, no. 3, pp. 244–256, 2024, doi: 10.1515/jisys-2023-0012.

[12] L. Santoso and R. Hartati, "Evaluation of Trade-offs in Fraud Detection Models," *Indones. J. Comput. Sci.*, vol. 17, no. 2, pp. 144–152, 2023, doi: 10.1234/ijcs.v17i2.456.

[13] D. Tanoto, A. Jatmiko, and H. Arifianto, "Benchmarking Machine Learning and Rule-Based Fraud Models," *J. Sist. Cerdas*, vol. 5, no. 2, pp. 67–78, 2023, doi: 10.5678/jsc.v5i2.789.

[14] Y. Vivek, V. Ravi, A. A. Mane, and R. Naidu, "Explainable Artificial Intelligence and Causal Inference Based ATM Fraud Detection," arXiv preprint, arXiv:2211.10595, Nov. 2022. [Online]. Available: https://arxiv.org/abs/2211.10595

[15] Y. Vivek, V. Ravi, A. A. Mane, and R. Naidu, "ATM Fraud Detection Using Streaming Data Analytics," arXiv preprint, arXiv:2303.04946, Mar. 2023. [Online]. Available: https://arxiv.org/abs/2303.04946