Jurnal Nasional Teknik Elektro dan Teknologi Informasi
Volume 14 Number 2 May 2025

DOI: 10.22146/jnteti.v14i2.17410

Detecting Fraudulent Transaction in Banking Sector Using Rule-Based Model and Machine Learning

Cut Dinda Rizki Amirillah

Computer Science Program, School of Computer Science, Bina Nusantara University, Jakarta Barat, DKI Jakarta 11530, Indonesia

[Received: 18 November 2024: Revised: 22 January 2025, Accepted: 16 April 2025]
Corresponding Author: Cut Dinda Rizki Amirillah (email: cut.amirillah@binus.ac.id)

ABSTRACT — This research aims to develop an effective fraud detection model in banking transactions using the rule-based model (RBM) approach and the isolation forest (IF) machine learning algorithm. Based on data from the Ministry of Communication and Information Technology, there were more than 405,000 online fraud cases during the 2019–2022 period, indicating the need for a reliable fraud detection system to protect customers. The research method involves collecting banking transaction data for four months through channels such as ATM, internet banking, and mobile banking. The RBM model was used as an initial approach, detecting suspicious transaction patterns based on defined rules. However, it has limitations in detecting transactions that are not defined in the rules. To complement this shortcoming, this research implemented IF, an effective unsupervised learning model for detecting anomalies using the isolation tree (iTree) technique to identify suspicious transactions. The results showed that the IF model could detect anomalous patterns not covered by RBM, thereby improving the accuracy of fraud transaction identification. The precision data of 99% indicates that the model's predictions of anomalies are indeed anomalies, while a recall value of 1.0 shows that the model successfully identified all anomalies in the dataset. In conclusion, the combination of RBM and IF provides a comprehensive approach to fraud detection in the banking sector. IF's ability to detect anomalies more dynamically and accurately can reduce fraud losses in the industry.

KEYWORDS — Machine Learning, Isolation Forest (IF), Rule-Based Model (RBM), Banking Sector.

I. INTRODUCTION

According to the Ministry of Communication and Information, from 2019 to 2022, approximately 486,000 cases of fraud were documented. Among these cases, online fraud was the most prevalent, with 405,000 reports. It is crucial to note that small-scale fraud acts can lay the groundwork for more significant fraudulent activities, resulting in a broader impact that ranges from embezzlement of substantial funds to the misuse of debtor credit, which can prove detrimental to banks [1]. In Indonesia, regulators like Bank Indonesia and the Financial Services Authority have established guidelines to implement anti-fraud strategies for banks. These regulations, outlined in Financial Services Authority Regulation (Peraturan Otoritas Jasa Keuangan, POJK) Number 39/POJK.03/2019 [2] and Bank Indonesia Number 23/6/PBI/2021 [3], specifically address payment service providers. Financial service providers are mandated to adopt an anti-fraud system, with the fraud detection system being a key component. This system incorporates a rule-based model (RBM) functioning as a data filter before processing. While conventional methods are still useful, they are considered less effective in detecting massive transactions in the banking sector [4].

Fraud is a comprehensive term referring to actions aimed at obtaining financial benefits through illegal and fraudulent methodologies across various sectors, including insurance, banking, taxation, and the corporate domain [5]. The fraud triangle, a model delineating conditions that heighten the likelihood of fraud, has been conceptualized by researchers [6], and the Association of Certified Fraud Examiners (ACFE) [7]. Pressure involves situations where an individual has an initial motivation to engage in fraudulent activities. Opportunities are circumstances exploited by criminals to commit fraud, and rationalization is the stage when the perpetrator convinces themselves that their actions are justified, thereby diminishing feelings of guilt. Currently, banks have a fraud detection system to capture suspicious data based on an RBM. RBM represents an approach used to detect fraudulent transactions [8]. Each rule is endowed with a threshold, parameterized or adjustable to meet the bank's requirements. The categories of RBM, along with the thresholds for identifying suspicious transactions, are outlined in Table I.

Financial behavior is designed to capture patterns of financial transactions that occur repeatedly in a short period with unusual amounts. User behavior is a rule designed to detect repeated login activities and balance checks within close time intervals. Multiple accounts are designed to identify 1-to-many patterns where one account sends transactions to multiple accounts simultaneously. The implementation of RBM has several significant advantages in detecting fraudulent transactions. However, this RBM has a weakness: transactions with anomalies beyond the set threshold cannot be captured by the fraud detection system application. Therefore, a machine learning method is needed to predict fraudulent transactions [9]. Efficient processing of large datasets necessitates adopting a machine learning approach over conventional RBM. In the development of machine learning models for fraud detection, these models are generally using classification. Classification models aim to distinguish transactions as fraudulent or nonfraudulent, providing an effective means to determine suitable methods for financial fraud detection [10].

Machine learning, a facet of artificial intelligence, focuses on developing algorithms and statistical models enabling computers to learn from data and making predictions or decisions based on identified patterns [11]. It serves as an analytical technique capable of uncovering patterns without requiring manual guidance from an expert [12]. In the banking

TABLE I
RULE-BASED MODEL (RBM)

No	Category	Threshold
1	Financial behavior	Total amount, range time, frequency
2	User behavior	Frequency of login, balance inquiry attempt
3	Multiple account	One to many transactions, number of destination account

industry, it can enhance fraud detection by analyzing extensive data to identify patterns unattainable with conventional RBM. This research employed unsupervised learning, a machine learning model particularly adept at detecting anomalous transactions, revealing patterns and anomalies indicative of fraudulent behavior. This enables businesses to detect and prevent fraud in real-time, minimizing false alerts and enhancing security [13].

Isolation forest (IF), an unsupervised learning method, comprises a collection of isolation trees (iTrees) derived from a specific dataset to detect anomalies in identifying fraudulent transactions [14]. Anomaly detection with IF involves two stages. The initial stage is the training stage, constructing an iTrees using a subsample of the training dataset. The subsequent testing stage assigns test instances to the iTrees, yielding anomaly values for each instance [15].

The urgency of this research lies in the increase of fraud cases that are increasingly complex and have a significant impact on the stability of the banking sector. By adopting machine learning methods, especially those based on unsupervised learning, it is expected that fraud detection can be carried out more effectively and in a timely manner, thereby minimizing greater financial losses and maintaining the integrity of the banking system.

Previous studies focused on fraud detection using RBM and other traditional methods, emphasizing their efficiency in identifying specific anomalies but highlighting their shortcomings in scalability and flexibility [5]. Meanwhile, emerging research explored machine learning approaches, particularly classification models, to enhance detection accuracy and identify fraudulent activities dynamically [6]. However, these studies often concentrated on supervised learning, requiring labeled datasets, which can be challenging to obtain in real-world scenarios.

This study addressed these gaps by adopting an unsupervised learning approach, specifically the IF, to improve fraud detection in banking transactions. The IF method has shown promise in detecting anomalies through its unique structure of iTrees, which efficiently isolates outliers from the data [7]. Unlike supervised models, the IF method does not require labeled data, making it highly applicable to banking datasets with minimal prior classification.

The novelty of this research lies in integrating an unsupervised learning model with traditional RBM to develop a hybrid framework capable of addressing the limitations of each approach. By leveraging the strengths of machine learning, this study contributes to the development of a scalable, adaptive, and robust fraud detection system tailored to the dynamic nature of financial transactions.

The significance of this research lies in its potential to mitigate financial losses and bolster the stability of the banking sector. As fraud cases become increasingly complex and impactful, the adoption of advanced detection systems is crucial for safeguarding financial institutions and enhancing public trust. Moreover, this study provides a roadmap for financial service providers to transition from conventional detection models to artificial intelligence (AI)-driven solutions, ensuring real-time fraud prevention and minimizing false positives.

II. RELATED WORKS

The current banking landscape and implementing fraud detection are crucial for safeguarding financial transactions [16]. At its core, this system relies on an RBM approach where each rule is equipped with a threshold, a parameter finely tuned to align with the specific risk tolerance and requirements of the banking institution. These rules act as "vigilant gatekeepers," systematically analyzing incoming data to identify and flag transactions displaying characteristics indicative of fraudulent activities. The structured nature of the RBM ensures a rapid response to potential threats, thereby enhancing the overall security of financial transactions [17]. Despite its effectiveness, the RBM has inherent limitations, notably its rigidity, meaning that transactions with anomalies beyond predefined thresholds may escape detection. This limitation necessitates a more adaptive and sophisticated solution, leading to the integration of machine learning into fraud detection.

Machine learning introduces a dynamic and learning-oriented paradigm, enabling the system to evolve and adapt to the ever-changing patterns in financial transactions [18]. By leveraging machine learning models, the fraud detection system gains the capacity to predict and identify fraudulent activities that might elude traditional RBM. When delving into the intricacies of machine learning models for fraud detection, two primary categories emerge: classification and regression models [19]. Classification models excel at distinguishing transactions as either fraudulent or nonfraudulent, offering a powerful tool for discerning effective methods in the financial fraud detection landscape [20]. On the other hand, regression models delve into uncovering correlations between variables that may contribute to a transaction being classified as fraudulent.

The use of machine learning techniques not only enhances the overall efficacy of the fraud detection system but also empowers it to adapt to intricate and evolving patterns of fraudulent activities [21]. The continuous evolution of financial landscapes underscores the importance of the symbiotic relationship between RBM and machine learning IF capabilities in fortifying defenses against the ever-persistent threat of financial fraud. As institutions embrace this hybrid approach, they position themselves at the forefront of innovation and resilience in the face of an evolving threat landscape.

A. RULE-BASED MODEL

According to prior research, fraud must be actively hunted and detected as early as possible [9]. This becomes even more crucial when attempting to use supervised methods for fraud detection. One suitable method is the use of an RBM. Such a system matches each data with a set of predetermined indicators. The aim of the study is to detect fraudulent cases which occur in telecommunication networks and identify anomalies in health insurance claim processes or warn against fraud in consumer credit. The process of training the RBM involved not only traditional numeric features, but also textual

features extracted from descriptions through text processing algorithms such as latent Dirichlet allocation.

In another study related to RBM, research was conducted to detect anomalous credit card transactions using the anomalous pattern and transaction examination (APATE) method, a new approach to detect credit card transaction fraud in online stores [8]. The approach combined (1) intrinsic features obtained from incoming transaction characteristics and customer spending history using recency–frequency–monetary (RFM) basics; and (2) network-based features by leveraging the credit cardholder and merchant networks, obtaining suspicion scores dependent on time for each network object. The results indicated that intrinsic and network-based features are closely interrelated in the same context. The combination of these two types of features produced the best-performing model with an area under the curve (AUC) score exceeding 0.98. From these two studies, it can be concluded that a RBM is a viable method for detecting fraudulent transactions by setting a threshold that can be adjusted by the user. However, in the last decade, detection methods can also be carried out by machine learning.

B. MACHINE LEARNING

Previous research utilizing a machine learning model identified several factors influencing the performance of the IF in detecting fraudulent transactions on credit card channels [22]. There are four experimental scenarios: an analysis of the influence of split ratio on validation data, the impact of feature selection, the effect of the number of fraudulent data in the training set, and the adjustment of hyperparameter values [10]. The statement outlines a research study that employed a machine learning model, specifically the IF, to detect fraudulent transactions in banking sector. The research aimed to understand and evaluate the factors affecting the model's performance. Overall, the study aimed to provide insights into the optimal configuration and conditions for the IF to enhance its efficacy in identifying fraudulent transactions on credit card channels [23].

Another study has demonstrated the application of the IF for detecting anomalies and other rare events, such as fraud. The results indicated that tuning the IF can yield significant improvements in traditional classification metrics, such as AUC, as well as unconventional metrics that may be relevant to businesses with limited resources [24]. Comparisons with clustering approaches also have a similar impact, illustrating how both options are beneficial for exploring anomaly detection and how the results of the IF potentially make it easier to interpret across the entire dataset. Overall, the paper highlights the effectiveness of the IF in detecting anomalies, particularly in cases like fraud, and emphasizes its potential advantages, including improved classification metrics and ease of interpretation across diverse datasets [25].

III. METHODOLOGY

The literature review was conducted by exploring various sources discussing fraud detection. Additionally, this study examined relevant prior research. Two approaches were used in detecting fraudulent transactions: the first approach utilized RBM [8], while the second approach adopted the IF machine learning method [24].

The first approach, which involved identifying fraud using RBM in banking transactions, relies on rules to recognize suspicious or unusual patterns. However, this approach has limitations as it is restricted to detecting suspicious transactions predefined within the rules. Therefore, the second approach, employing IF, is necessary [25].

The research began by collecting datasets from banking activities over a four-month period. The first selected method was the RBM, where RBM logic was utilized to detect transaction patterns. Meanwhile, the second method involved the implementation of IF, which underwent several data preprocessing stages, including data cleaning, processing, and preparation for use in the model [26]. Subsequently, the IF process was conducted, where the model was trained with the dataset and training data to detect anomaly patterns in the data. The results of the IF process were then evaluated and analyzed to identify transactions suspected of being fraudulent.

The subsequent step involved an in-depth analysis of the detected fraud. The banking data analysis process commenced with the collection of a dataset that covered banking activities over a four-month period. This dataset became the foundation for building two main models, namely RBM and IF.

In the RBM development stage, the dataset was processed using rule-based logic to produce an output called the rule-based result. Meanwhile, in the IF development, the data went through a preprocessing process that included data cleaning, processing, and preparation. Once the data were ready, the IF algorithm was applied to process the dataset and generate the isolation forest result. Next, the results of both models, namely the rule-based result and the IF result, were combined to build a final model called RBM + IF combination. This combined model was subsequently evaluated to measure its performance and validity. Based on the evaluation results, the final outcome of the model was presented as the main output.

This process was designed to improve accuracy and efficiency in analyzing banking activity data by utilizing the advantages of each approach, namely rule-based logic and anomaly detection using IF.

A. DATASET

This research utilized a dataset of banking transactions over four months. The data were extracted from a mirroring database provided by the bank, containing transaction data on online channels such as ATMs, internet banking, and mobile banking. The data were then filtered into a relevant transaction table for bank transaction data analysis. The data population in this study included transactions from April 19, 2023, to August 31, 2023, with a total of 2,968,228 rows, adhering to the following criteria:

1. from the master data's 29 columns, only 17 columns were used for this research;
2. only financial transaction data were used; nonfinancial data, such as balance inquiries, login activities, logout, or profile changes, were not included;
3. only transactions with successful response statuses were used; data with failed responses, such as timeouts or insufficient balances, were not included in the study;
4. transaction data was carried out on online channels, including ATMs, internet banking, as well as mobile banking.

Based on these data, transaction data features were selected for the datasets. This data feature selection resulted in 18 transaction data features and 1 class feature, as the classification result of transactions indicated as fraud. Detailed features can be seen in Table II.

TABLE II
DATASET STRUCTURE

No	Category	Description	Value
1	trkey	Reference number	341505001
2	accountIssuer	Account number issuer	1001568667
3	accountDestination	Destination account number	1002158333
4	trtime	Date and time of the transaction	2023-04-22 18:44:50.
5	merchant	Channel of the transaction	6410
6	amount	Amount of transaction	90000000
7	trtype	Transaction type	6011
8	trdesc	Transaction description	BI-FAST
9	financial	Financial flag	Y
10	trdescdetail	Transaction detail	BI-FAST Posting
11	responsecode	Transaction responses (success/failed)	0
12	responseaction	Response action	Successful Transaction
13	merchantdesc	Description of channel	Mobile Banking
14	destinationbank	Destination bank	ZYZ
15	issuerbank	Issuer bank	XYZ
16	acqbank	Acquiring bank	XYX
17	scenario	Classification of transaction frauds (fraud/normal)	1TOMANY
18	class	Reference number	1 / -1

B. RULE-BASED MODEL

The RBM method employs a set of predefined rules or conditions to identify patterns indicating fraud in banking transactions [8]. The process of fraud detection based on RBM involves several main steps to quickly and efficiently identify suspicious transactions [9]. Data sources collected from various channels were stored in a mirroring database set up in real-time mode. A logic engine utilizing Java Spring Boot implemented preestablished rules set by the bank, with each rule having a threshold to determine suspicious transaction. These thresholds were dynamic, allowing bank users to adjust them according to current fraud trends or business needs. The rules were designed considering common fraud patterns. The following are the rules and thresholds applied in this study.

1. Financial behavior had three main parameters as thresholds: the amount, frequency, and time interval. The time interval threshold was set to 1 minute, the frequency to 5 transactions, and the nominal threshold to IDR15,000,000. Thus, if a transaction is equal to or exceeds IDR15,000,000, or if there are more than 5 repeated transactions within a 1-minute interval, it will trigger the financial behavior scenario.
2. User behavior was designed with a threshold of suspicious login attempts, set at 4 times within a 1-minute interval. This rule enables the model to effectively capture suspicious user behavior.
3. Multiple accounts were designed to identify the 1-to-many pattern. By setting a threshold of 5 recipient accounts within a 1-minute interval, attempts at fraud involving unusual fund transfers can be detected.

C. MACHINE LEARNING

First, the necessary libraries were imported, including Pandas and NumPy for data processing, Matplotlib and Seaborn for data visualization, psycopg2 and SQLAlchemy for SQL connections, and ColumnTransformer for feature preprocessing using techniques like BinaryEncoder, StandardScaler, and OneHotEncoder.

1) DETERMINING OUTLIERS

The outlier function calculates outliers from a dataset [14]. It computed the first quartile (q1), second quartile (q2), and third quartile (q3). Then, the interquartile range (IQR) was used to calculate the lower bound (*min_IQR*) and upper bound (*max_IQR*) to determine outliers. The function iterated through each element of the dataset to check whether the value was an outlier or not. The results were displayed in terms of column name, lower bound, number of lower outliers, number of upper outliers, and a list of outliers.

2) DETERMINING NORMAL BOUNDS

The "normal" bounds were used to test if a variable followed a normal distribution. The test results were printed along with the null hypothesis (H0) and alternative hypothesis (Ha) [27]. If the *p*-value from the normality test was less than or equal to 0.05, then the null hypothesis (normal transactions) was rejected.

3) DATA COLLECTION AND PREPARATION

The "data_collected" function printed information about the collected data, including start date, end date, and the number of data points. The "data_prep" function prepares the data by performing several transformations, such as removing duplicates, changing data types, and extracting additional information from the time column.

The preparation steps for building and training the IF included loading data from two different CSV files into dataframes. The preprocessing process involved filling missing values in the "accountDestination" column with the string "na." After that, rows with values matching the regex pattern [A-Z+] in the "accountDestination" column were removed from the dataframe. The "drop_exclude()" function was then used to exclude rows with values in the "merchant" column already included in the list, and the "modify_trx_amount()" function was used to change values in the 'amount column according to certain conditions. The final step prepared the data using the "data_prep()" function, which changed data types and extracted additional information from the time column.

4) THE PIPELINE

It consists of two steps: the preprocessor for data transformation and "clf_iso" to set the IF as the classifier. In the first step of the pipeline, all previously defined transformers in the preprocessor were applied to the input data before the model was trained. These transformers included OneHotEncoder, BinaryEncoder, StandardScaler, and TfidfVectorizer. After processing through these transformers, the data were ready for further processing by the model. In the subsequent step of the pipeline, the IF was built with predefined hyperparameters. The *n_estimators* was set to 100 to determine the number of trees to be built in the ensemble, contamination was set to 0.01 to control the expected proportion of outliers in the data, and *random_state* was set to 42 to set the random initialization value, crucial for result reproducibility. After creating the pipeline, "model.fit(df[relevant_features])" was used to train the model on the input data. The data used for training were a subset of the dataframe "df" consisting only of columns deemed relevant for model training, as determined in the *relevant_features* variable. Once the model was trained, predictions were made on the same data to determine whether each data row was considered an outlier or not. Subsequently, the prediction results were then stored in a new column named "ai_behavior" in the dataframe "df." Therefore, each data row was labeled as normal (1) or abnormal (-1) based on the model's prediction.

IV. RESULTS AND DISCUSSION

A. DATASET

From the provided dataset collected over a span of four months from online channels such as ATMs, mobile banking, and internet banking, the machine learning model predicted 2,938,545 transactions as normal and 29,683 transactions as fraud. On the other hand, RBM predicted 2,730,130 transactions as normal and 208,415 transactions as fraud. The combination of machine learning and RBM methods predicted 2,966,473 transactions as normal and 1,755 transactions as fraud. Table III shows the data comparison of normal and fraud categories.

B. EVALUATION METHOD

This study utilized a confusion matrix to evaluate the model's performance. The accuracy and prediction precision could be determined by comparing the number of observations classified correctly and incorrectly. These data were then used to calculate metrics, including accuracy, precision, recall, and F1 score, using commonly used formulas, including from [20]. The explanation of these formulas is presented as follows:

$$Accuracy = \frac{TP+TN+FP+FN}{TP+TN}. \quad (1)$$

A true positive (*TP*) indicates the number of positive samples that are correctly predicted by the model. The number of negative samples incorrectly predicted by the model as positive sample is known as a false positive (*FP*), while a false negative (*FN*) is the number of positive samples mistakenly identified by the model as negative. A true negative (*TN*) is the number of negative samples correctly identified by the model as negative [15].

C. RESULT ANALYSIS

Based on Figure 1, the precision data of 99% indicates that the model's predictions of anomalies are indeed anomalies, while a recall value of 1.0 shows that the model successfully identifies all anomalies present in the dataset. The evaluation results of the RBM are shown in Figure 1(b). The model yielded an accuracy of 86.78%, indicating the level of agreement between correct predictions and total samples. However, the low precision of 32.83% indicates that only a small portion of positive predictions are correct, while the high recall of 100% shows that the model successfully detects all true positive samples. The F1 score, which is the average of precision and recall, yielded a moderate value of 49.44%, reflecting the balance between precision and recall. In addition, Figure 1(b) indicates that the model predicted 1,919,876 (80.32%) data as TN and 154,435 (13.22%) instances as TP, no instances were predicted as FN. However, there were 315,866 (6.46%) instances predicted as FN.

This model showed a tendency to always predict the positive class, failing to detect the negative class. This suggests an imbalance or problem in negative classification, which could lead to errors if negative class data is essential to identify in real applications.

TABLE III
COMPARISON OF NORMAL AND FRAUD

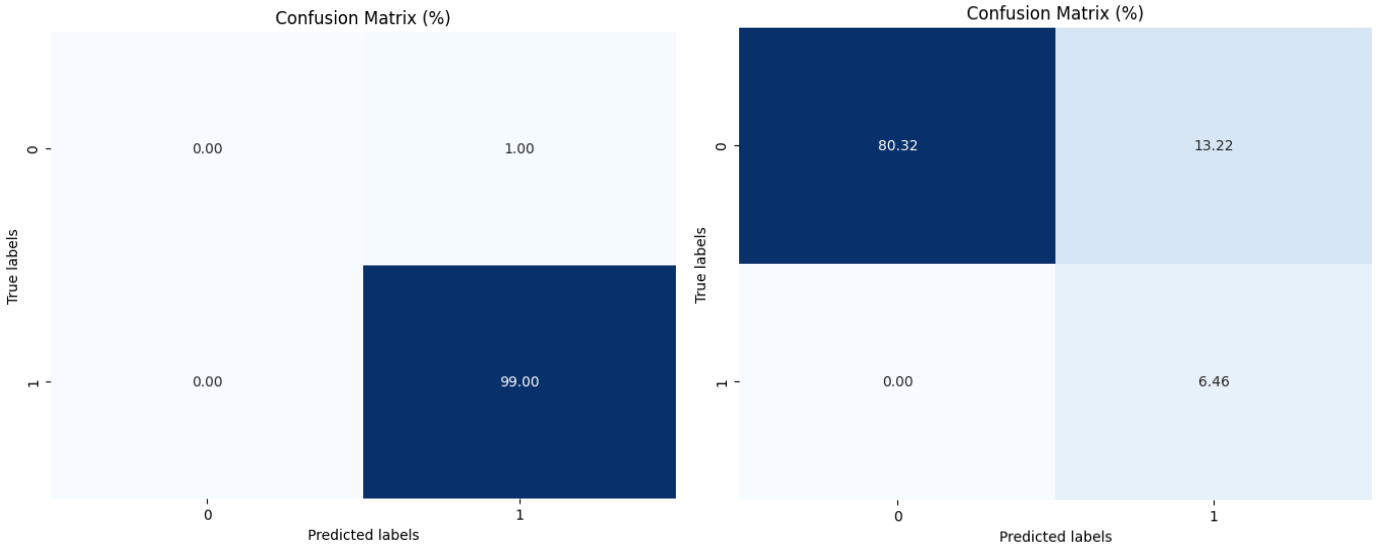
Prediction	RBM	IF	RBM + IF
Normal	2,938,545	2,730,130	2,966,473
Fraud	29,683	208,415	1,755

D. COMPARISON WITH EXISTING METHODS ANALYSIS

Table IV presents the performance evaluation results of three different classification models: RBM, machine learning, and a combination of both (RBM + machine learning). The columns show performance evaluation metrics including accuracy, precision, recall, and F1 score. The RBM model achieved an accuracy of 87% and a precision of 33%, indicating the model's ability to accurately identify positive instances out of all predicted positive instances. Despite achieving a recall of 100%, the F1 score only achieved 49%, indicating an imbalance between precision and recall. Conversely, the machine learning model exhibited a very high accuracy and precision; nonetheless, its F1 score was 0.0% due to achieving 100% in recall, indicating failure to classify negative instances. Table IV shows a comparison of the performance results of the suspicious transaction detection model proposed in this study with previous methods used in related research. This comparison includes several key evaluation metrics, namely accuracy, precision, recall, and F1 score, which are common indicators in measuring the effectiveness and accuracy of detection models. Some methods, such as the IF model developed by [24] and the RBM used by [8] with PaySim and BankSim datasets, are presented as references to see performance comparisons. In [24], the IF recorded a total of 71 errors, with the accuracy of 99.72%; whereas the local outlier factor recorded a total number of 107 errors and an accuracy of 99.62%. Meanwhile, this study tested the performance of the IF model and RBM, both individually and combined RBM + IF). Based on the table results, the combined RBM + IF shows comparable or even better performance in several aspects than the previous methods, especially in terms of accuracy (99.98%) and precision (100%), thus strengthening the potential of this model in detecting suspicious transactions more effectively.

V. CONCLUSION

Mobile banking, and internet banking, the combination of two models, RBM + IF, has proven to yield a high level of



(a) (b)

Figure 1. Comparison confusion matrix, (a) IF and (b) RBM.

TABLE IV
COMPARISON WITH EXISTING METHODS

Reference	Model	Accuracy (%)	Precision (%)	Recall (%)	F1 Score (%)
[24]	IF (0)	99.62	1.00	1.00	1.00
	IF (1)		0.28	0.29	0.28
[8]	Rule base (PaySim)	99	99	98	98
	Rule base (BankSim)	99	99	98	98
This Paper	RBM	87	33	100	49
	IF	99	98	100	0.0
	RBM + IF	99.98	100	99	99

accuracy to detect suspicious transactions in a banking environment, particularly those from online channels such as ATMs. This can be a consideration for banks to conduct fraud detection quickly and accurately. The evaluation of this research indicated that the combination of RBM and IF yielded the best performance with high values in accuracy, precision, reca ll, and F1 score. The RBM achieved perfect recall but low precision, whereas the IF achieved high precision but a low F1 score due to its poor recall. The combination of both models overcomes the weaknesses of each model and produces a balanced performance with excellent performance in all evaluation metrics.

In the RBM implementation, adding new scenarios related to internal fraud committed by bank personnel is recommended. IF can recommend new rules based on learning from data and current fraud trends. Additionally, the RBM can be used to recommend whether transactions should be analyzed as fraudulent or normal based on the results of the existing RBM. Utilizing this approach, it is hoped to improve the accuracy and effectiveness of fraud detection systems in identifying suspicious transactions and reducing the impact of financial crime activities in the future.

CONFLICTS OF INTEREST

The author declares that there is no conflict of interest.

REFERENCES

[1] B.H. Reddy and N.T. Rao, "Fraud Detection in Financial Transactions", *Int. J. Eng. Res. Sci. Technol.*, vol. 20, no. 4, pp. 92-98, Nov. 2024.

[2] "Penerapan Strategi Anti Fraud bagi Bank Umum," Peraturan Otoritas Jasa Keuangan, No. 39/POJK.03/2019, 2019.

[3] "Penyedia Jasa Pembayaran," Peraturan Bank Indonesia, No. 23/6/PBI/2021, 2021.

[4] A. Olushola and J. Mart, "Fraud detection using machine learning," Jan. 2024.

[5] E.R. Kismawadi, U.D.A. Muddatstsir, and A. Hamid, *Fraud pada Lembaga Keuangan dan Non Keuangan.* Depok, Indonesia: PT. RajaGrafindo Persada, 2020.

[6] R. Abdulahi and N. Mansor, "Fraud triangle theory and fraud diamond theory. Understanding the convergent and divergent for future research," *Int. J. Acad. Res. Account. Finance Manag. Sci.*, vol. 5, no. 4, pp. 54–64, Dec. 2015, doi: 10.6007/ijarafms/v5-i4/1823.

[7] ACFE Indonesia Chapter, "Survei Fraud Indonesia 2019," 2020. [Online]. Availabe: https://acfe-indonesia.or.id/wp-content/uploads/2021/02/SURVEI-FRAUD-INDONESIA-2019.pdf

[8] S. Islam, M.M. Haque, and A.N.M.R. Karim, "A rule-based machine learning model for financial fraud detection," *Int. J. Electr. Comput. Eng. (IJECE)*, vol. 14, no. 1, pp. 759–771, Feb. 2024, doi: 10.11591/ijece.v14i1.pp759-771.

[9] M. Baumann, "Improving a rule-based fraud detection system with classification based on association rule mining," in *Proc. Ges. Inform.*, 2021, pp. 1121–1134, doi: 10.18420/informatik2021-091.

[10] S. Adewale and A.B. Madu, "Credit card fraud detection using machine learning," unpublished.

[11] I. Nwade *et al.*, "Development of credit cards fraud detection model," *LAUTECH J. Eng. Technol.*, vol. 17, no. 2, pp. 1–8, 2023.

[12] M.G. Saragih *et al.*, "Machine learning methods for analysis fraud credit card transaction," *Int. J. Eng. Adv. Technol. (IJEAT)*, vol. 8, no. 6S, pp. 870–874, Aug. 2019, doi: 10.35940/ijeat.F1164.0886S19.

[13] A. Bănărescu, "Detecting and preventing fraud with data analytics," *Procedia Econ. Finance*, vol. 32, pp. 1827–1836, 2015, doi: 10.1016/s2212-5671(15)01485-9.

[14] M. Pełka and A. Dudek, "Isolation forests for symbolic data as a tool for outlier mining," *Econom., Ekonom., Adv. Appl. Data Anal.*, vol. 28, no. 1, pp. 1–10, Jan. 2024, doi: 10.15611/eada.2024.1.01.

[15] M.K.M. Almansoori and M. Telek, "Anomaly detection using combination of autoencoder and isolation forest," in *1st Workshop Intell. Infocommunication Netw. Syst. Serv. (WI2NS2)*, 2023, pp. 25–30, doi: 10.3311/wins2023-005.

[16] A. Nursanti and I. Trinugroho, "The effect of financial literacy on the ability to detect investment fraud," *Int. J. Soc. Sci. Res. Rev.*, vol. 6, no. 12, pp. 323–337, Dec. 2023, doi: 10.47814/ijssrr.v6i12.1840.

[17] K.F. Andriani, K. Budiartha, M.M.R. Sari, and A.A.G.P. Widanaputra, "Fraud pentagon elements in detecting fraudulent financial statement," *Linguist. Cult. Rev.*, vol. 6, pp. 686–710, Jan. 2022, doi: 10.21744/lingcure.v6ns1.2145.

[18] M. Sirigineedi *et al.*, "Fake credit transaction detection using machine learning," *Int. J. Res. Sci. Eng.*, vol. 4, no. 3, pp. 1–9, Apr./May 2024, doi: 10.55529/ijrise.43.1.9.

[19] E. Pan, "Machine learning in financial transaction fraud detection and prevention," *Trans. Econ. Bus. Manag. Res.*, vol. 5, pp. 243-249, Mar. 2024, doi: 10.62051/16r3aa10.

[20] H. Kamel and M.Z. Abdullah, "Distributed denial of service attacks detection for software defined networks based on evolutionary decision tree model," *Bull. Electr. Eng. Inform.*, vol. 11, no. 4, pp. 2322–2330, Aug. 2022, doi: 10.11591/eei.v11i4.3835.

[21] N.S. Arunraj *et al.*, "Comparison of supervised, semi-supervised and unsupervised learning methods in network intrusion detection system (NIDS) application," *AKWI*, no. 6, pp. 10–19, Dec. 2017, doi: 10.26034/lu.akwi.2017.3183.

[22] G.M. Rao and D. Ramesh, "Ranger random forest-based efficient ensemble learning approach for detecting malicious URLs," in *Proc. Int. Conf. Recent Trends Mach. Learn. IoT Smart Cities Appl.*, V.K. Gunjan and J.M. Zurada, Eds., 2020, pp. 599-608, doi: 10.1007/978-981-15-7234-0_56.

[23] M.I. Akazue *et al.*, "UNMASKING FRAUDSTERS: Ensemble features selection to enhance random forest fraud detection," *J. Comput. Theor. Appl.*, vol. 1, no. 2, pp. 201–211, Dec. 2023, doi: 10.33633/jcta.v1i2.9462.

[24] V. Vijayakumar, N.S. Divya, P. Sarojini, and K. Sonika, "Isolation forest and local outlier factor for credit card fraud detection system," *Int. J. Eng. Adv. Technol. (IJEAT)*, vol. 9, no. 4, pp. 261–265, Apr. 2020, doi: 10.35940/ijeat.D6815.049420.

[25] M.L.V. Nalupa, J.R.D. Fernandez, W.J.C. Dacay, and M.M. Bergado, "Fraud detection using isolation forest for RFID-based attendance monitoring system," *Sci. Int.*, vol. 6, no. 34, pp. 511-517, Dec. 2022.

[26] A. Zulfikar, F.A. Rahmani, and N. Azizah, "Deteksi anomali menggunakan isolation forest belanja barang persediaan konsumsi pada satuan kerja Kepolisian Republik Indonesia," *J. Manaj. Perbendaharaan*, vol. 4, no. 1, pp. 1–15, Jun. 2023, doi: 10.33105/jmp.v4i1.435.

[27] H. John and S. Naaz, "Credit card fraud detection using local outlier factor and isolation forest," *Int. J. Comput. Sci. Eng.*, vol. 7, no. 4, pp. 1060–1064, Apr. 2019, doi: 10.26438/ijcse/v7i4.10601064.