Comparative Assessment of Fraudulent Financial Transactions using the Machine Learning Algorithms Decision Tree, Logistic Regression, Naïve Bayes, K-Nearest Neighbor, and Random Forest

Paiboon Manorom
Department of Information Science, Faculty of Humanities and Social Sciences, Khon Kaen University, Thailand
paiboon.m@kkumail.com

Umawadee Detthamrong
College of Local Administration, Khon Kaen University, Thailand
umadet@kku.ac.th

Wirapong Chansanam
Department of Information Science, Faculty of Humanities and Social Sciences, Khon Kaen University, Thailand
wirach@kku.ac.th (corresponding author)

Received: 8 May 2024 | Revised: 28 May 2024 | Accepted: 12 June 2024

Licensed under a CC-BY 4.0 license | Copyright (c) by the authors | DOI: https://doi.org/10.48084/etasr.7774

ABSTRACT

Today, fast-paced technology plays an important role in financial transactions, especially in payment-related digital habits. As fraud is a major concern in online payments, many machine-learning approaches have been proposed to detect and prevent fraudulent payment transactions. This study aimed to evaluate Decision Tree, Logistic Regression, Naïve Bayes, K-Nearest Neighbor, and Random Forest in detecting fraudulent payment transactions. The results show that Random Forest, K-Nearest Neighbor, Decision Tree, and Logistic regression achieved total accuracy rates exceeding 99%. However, such impressive results do not necessarily indicate satisfactory performance. The results highlight the need to detect fraudulent transactions and investigate specific improvements to effectively manage and minimize unexpected financial transaction fraud.

Keywords- machine learning algorithms; data mining; customer payment transaction; data analytics

I. INTRODUCTION

Today, several innovative digital technologies entail a variety of new livelihoods, lifestyles, societal phenomena, and modern commerce, especially in digital payments. Novel digital banking technology and payment methods have significantly changed business management, particularly credit card payment. Traditional cash and check payments are replaced by a variety of digital, contactless, and mobile payment solutions driven by technological advances, changes in consumer behavior, and the need for improved efficiency [1]. Consumers have consistently moved away from traditional transactions and adjusted their way to fit with digital payments. Since digital payments could lead to fast payment and convenience, digital payments through mobile or websites have become a daily life habit [2]. In this context, staying attuned to the latest payment trends is not just a matter of convenience but a fundamental necessity for businesses to succeed in the digital age. Credit and debit cards were the fastest banking services for purchasing products, online or on-site [3, 4]. However, the risk of fraudulent card transactions is an inevitable consequence.

Credit card fraud tends to increase significantly [5-7]. This entails significant and increasing financial losses for both customers and financial industries worldwide. As a result, financial businesses around the world face challenges with fraudulent transactions, especially with online credit card transactions. Consequently, financial and banking services need to employ state-of-the-art technology against financial cybercrimes, particularly machine learning, to detect, identify, and prevent both online and in-person fraudulent transactions [1, 8-12]. Several studies have recently investigated machine-learning approaches to improve fraud detection. In [8, 11, 12], machine-learning models were proposed and compared along with hyperparameter tuning. In [11], class weight hyperparameter tuning was used to control the weight of fraudulent and legitimate transactions and accelerate fraud detection and prevention using LightGBM, CatBoost, and XGBoost along with five-fold cross-validation. In [8, 12], machine-learning methods were proposed to reduce the cost of development in global banking services. The models proposed in [1, 9, 10] focused on genuine transactions instead of pattern matching or rule-based detection, which would cause missing occurrences. In addition, an exclusive algorithm may not be able to perform extensive analysis and detection with precise prediction capabilities, leading to shortcomings. These studies compared the performance of multiple algorithms in fraud detection. Furthermore, data mining approaches were used to analyze customer payment behavior and create policies and strategies based on relationships and categorization. Such approaches can reduce processing times and lead to precise customization and prediction to support and secure customer payments [13]. These approaches are considered essential tools to analyze customer purchasing behaviors and preferences, which are fundamental information for businesses to thrive steadily and survive in a rapidly changing economy.

This study aimed to:

- Compare five machine learning models to detect fraudulent purchasing transactions.
- Use multiple metrics to thoroughly evaluate their performance and efficacy.

II. THEORETICAL FRAMEWORK

In [14] the Cross-Industry Standard Process for Data Mining (CRISP-DM) was applied to investigate the relations of customer segmentation with the data and find customer preferences based on their transactions. Data mining refers to the process of searching and analyzing a large batch of raw data to identify patterns and extract useful information. Many businesses use data mining approaches to learn more about their customers and develop more effective marketing strategies, increase sales, and reduce costs. Several studies have used various data mining components. Data mining involves algorithms and techniques to convert large collections of data into useful output. The most popular data mining techniques are as follows [5].

- Decision Tree is a tree-based model for classification and regression. The model represents the data as a tree-like structure with specific features. This method is considered a crucial analysis process, as it helps to understand how the model makes predictions and provides insights into the relationships between the features and the target variable [15, 16].
- Logistic Regression (LR) is an algorithm for brief analysis and straightforward processing of class features, helping the analyst to explore the relationship among the variable and binary outcome, such as fraud and non-fraud. Prediction is used in a statistical sense with a specific model for which the variable is strongly, significantly, and independently associated with the outcome and therefore can be considered influential in the path to that outcome [17].
- Naïve Bayes is used to make decisions or predictions based on a set of rules or questions. It works for classification tasks as a fundamental probability theory concept to simplify assumptions for independent variables, features, or attributes [8].
- K-Nearest Neighbor is used for classification and regression problems in various fields, such as customer segmentation, recommendation systems, and discovering patterns and structures within datasets. This algorithm is a powerful tool for exploratory data analysis and can be a valuable step in preparing data for further analysis or machine learning tasks [18].
- Random Forest combines multiple decision trees to make a prediction. Random Forest is a popular machine-learning method for developing prediction models in many research settings. In prediction modeling, the goal is to reduce the number of variables needed to obtain a prediction, reduce the burden of data collection, and improve efficiency. RF can handle high dimensional data and complex relationships between features, making it a suitable choice for fraud detection tasks [16, 19].

This study used RapidMiner to analyze the data and apply the machine learning algorithms.

III. RESEARCH METHODOLOGY

Today, financial institutions need to secure customer transactions with highly effective measures. This study employed Decision Trees, Logistic Regression, Naïve Bayes, K-Nearest Neighbor, and Random Forest to detect fraudulent transactions. Several methods have been proposed for this purpose [1, 8-12]. In addition, machine learning can also assist financial institutions in customizing customer experiences using a large number of variables for strategic and policy decisions, marketing promotion, and customer behavior recognition.

A. Dataset

This study used a dataset containing a multi-agent virtual world simulation performed by IBM, covering 2000 (synthetic) consumers in the United States [20]. Data were collected from four financial service providers, namely Amex, Discover, Mastercard, and Visa, in the United States of America from 2002 to 2020. The dataset contains both credit and debit card transactions, covering several purchases and cards from consumers. The data analysis suggested that it is a reasonable match for real data in many dimensions, e.g., fraud rates, purchase amounts, Merchant Category Codes (MCCs), and other metrics. All columns, except the merchant name, have their natural value, which is helpful for feature engineering. The dataset was in a CSV format.

Missing data were removed. Unrelated data was also refined and revised to be compatible with the next steps. Table I shows a sample of the dataset consisting of 15 columns, without showing the columns labeled merchant code, error, and fraud. The dataset was split into an 80:20 ratio for training and testing. Table II shows the distribution of transactions in the dataset, and Table III details the selected features.

TABLE I. DATASET SAMPLE

User	Card	Year	Month	Day	Time	Amount	Use Chip	Merchant City	Merchant State	Zip	MCC
0	0	2002	9	1	06:21	$134.09	Swipe Transaction	La Verne	CA	91750	5300
0	0	2002	9	1	06:42	$38.48	Swipe Transaction	Monterey Park	CA	91754	5411
0	0	2002	9	2	06:22	$120.34	Swipe Transaction	Monterey Park	CA	91754	5411
0	0	2002	9	2	17:45	$128.95	Swipe Transaction	Monterey Park	CA	91754	5651
0	0	2002	9	3	06:23	$104.71	Swipe Transaction	La Verne	CA	91750	5912
0	0	2002	9	3	13:53	$86.19	Swipe Transaction	Monterey Park	CA	91755	5970
0	0	2002	9	4	05:51	$93.84	Swipe Transaction	Monterey Park	CA	91754	5411
0	0	2002	9	4	06:09	$123.50	Swipe Transaction	Monterey Park	CA	91754	5411
0	0	2002	9	5	06:14	$61.72	Swipe Transaction	Monterey Park	CA	91754	5411
0	0	2002	9	5	09:35	$57.10	Swipe Transaction	La Verne	CA	91750	7538
0	0	2002	9	5	20:18	$76.07	Swipe Transaction	La Verne	CA	91750	5814
0	0	2002	9	5	20:41	$53.91	Online Transaction	ONLINE			4900
0	0	2002	9	6	06:16	$110.37	Swipe Transaction	Mira Loma	CA	91752	5541
0	0	2002	9	7	06:16	$117.05	Swipe Transaction	Monterey Park	CA	91754	5411
0	0	2002	9	7	06:34	$45.30	Swipe Transaction	Monterey Park	CA	91755	5942

TABLE II. DATASET TRANSACTION DISTRIBUTION

Number of transactions	Legitimate transactions	Fraud transactions	Legitimate percentage	Fraud percentage
19,964	19, 937	27	99.86	0.14

TABLE III. DATA ATTRIBUTES FOR DATA ANALYSIS

Attribute	Description	Variable
Year	The year the transaction was made.	Integer
Card	Details on card type.	Integer
Payment method	Chip transaction, Swipe transaction, or Online transaction.	Integer
Error	Error in the payment, such as card expiration, CVV, technical glitch, PIN, insufficient balance, etc.	Integer
Amount	The amount in a particular transaction.	Numeric
Fraud	The fraud label in each transaction (Yes/No)	Integer

B. Performance Evaluation

Once the models were trained, their performance was evaluated in the testing dataset. This process was carried out to classify new input data using machine learning algorithms. The most common approaches to evaluate the classification performance of ML models are metrics based on the confusion matrix, as shown in Table III.

TABLE IV. CONFUSION MATRIX

		Transaction genuine class	
		P (Positive/Fraud)	N (Negative/No Fraud)
Predicted transaction class - Confusion	P	TP	FP
	N	FN	TN

The abbreviations in the confusion matrix are as follows: N denotes a Negative and P denotes a Positive, TN indicates True Negative (normal transaction classified as normal), FN indicates False Negative (fraud transaction classified as normal), FP denotes False Positive (normal transaction classified as fraud), and TP denotes True Positive (fraud transaction classified as fraud). Based on data from the confusion matrix, different metrics were calculated for binary classification performance [8, 11, 12]. However, highly unbalanced payment transaction data may be inconvenient. The precision and recall metrics were employed to evaluate the models.

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

$$Precision = \frac{TP}{TP+FP} \quad (2)$$

$$Recall = \frac{TP}{TP+FN} \quad (3)$$

C. Results

Table V shows the evaluation metrics per model. K-Nearest Neighbor and Random Forest achieved the highest accuracy of 99.87%, followed by Decision Tree and Logistic Regression with 99.86% and 99.82%, respectively. Naïve Bayes had the lowest accuracy of 94.14%. Tables VI and VII show more details on the performance of K-Nearest Neighbor and Random Forest.

TABLE V. EVALUATION OF MACHINE LEARNING ALGORITHMS

Criteria	Decision Tree	Logistic Regression	Naïve Bayes	K-Nearest Neighbor	Random Forest
Accuracy	99.86%	99.82%	94.14%	99.87%	99.87%
Precision	99.86%	99.87%	99.89%	99.87%	99.87%
Recall (Class No)	100%	99.95%	94.23%	100%	100%
Recall (Class Yes)	-	-	25.00%	-	-

TABLE VI. K-NEAREST NEIGHBOR RESULTS

	True No	True Yes	Class precision
Pred. No	5891	8	99.87%
Pred. Yes	0	0	0.00%
Class recall	100.00%	0.00%	

Accuracy: 99.87%

TABLE VII. RANDOM FOREST RESULTS

	True No	True Yes	Class precision
Pred. No	5891	8	99.87%
Pred. Yes	0	0	0.00%
Class recall	100.00%	0.00%	

Accuracy: 99.87%

IV. DISCUSSION

In [3], Random Forest was found to be the most appropriate machine learning algorithm to detect fraudulent credit card transactions. This study also showed that credit card holders over 60 years were found to be more susceptible to fraudulent transactions. In [9], Random Forest also showed good results in detecting fraudulent transactions. K-Nearest Neighbor and Random Forest can play a significant role in business models, not only for customer segmentations but also to help companies communicate promotions to customers. A strategic plan can be drawn to focus on revenue growth and retention, which are very important for business sustainability and stability. In these contexts, such models can provide critical views and benefits for companies. For retail banks, these models can be a guide to improve fraud detection algorithms, security, and management. Credit unions can also benefit from such algorithms for member management and protection from fraudulent transactions. Online banks and financial companies can also integrate such machine learning models to improve security and customer services. Payment processing companies can also use such algorithms to supervise electronic transactions to detect and prevent fraud. Investment banks and brokerage companies can use such algorithms to secure financial transactions. Insurance companies can also use such models to detect fraudulent claims or transactions related to insurance products. Mortgage lenders and loan providers could benefit from fraud detection capabilities for their loan repayment and disbursement processes [16, 18, 19, 21]. In summary, such approaches can benefit those involved in financial processing in any way and can be crucial in decision-making processes to protect against a large number of financial risks and improve the ability to manage customer affiliations [22-24].

However, the application of machine learning must be very careful. Although the overall accuracy of the models is satisfactory, most models were unable to detect fraudulent transactions. Specifically, although Naïve Bayes had the lowest accuracy, it was the only model to discover fraudulent transactions, even with a small recall rate. This highlights the necessity to examine multiple metrics when evaluating the performance of machine learning models. Class imbalances make total accuracy an inappropriate metric for evaluation, as the best-performing models in terms of total accuracy did not manage to detect any fraudulent transactions. This raises awareness for wider or deeper data, better pre-processing techniques, application of data augmentation methods, and more thorough performance evaluation. In addition, data analysis in a specific field may not be able to generalize. These models may be crucial for fraud detection, but they must be carefully applied to provide a satisfactory performance [25, 26]. Similar case studies can be carried out in other organizations, departments, or services in both the public and private sectors [27].

V. CONCLUSION

The results of this study show the importance of examining multiple metrics, such as accuracy rate, class precision, and class recall when evaluating machine learning models. In terms of total accuracy, all models achieved impressive accuracy, with the K-Nearest Neighbor and Random Forest achieving 99.87%, followed by the Decision Tree and Logistic regression with 99.86 % and 99.82%, respectively. However, these models did not manage to detect fraudulent transactions. On the other hand, Naïve Bayes had the lowest overall accuracy (94.14%) but was the only model that detected some fraudulent transactions. Machine learning algorithms can effectively assist in fraud detection [1, 6, 7, 21]. However, their application requires in-depth performance evaluation along with suitable pre-processing techniques to deal with class imbalances. In addition, this indicates the need to use multiple datasets.

Improving classification methods for fraud detection, which is a delicate application and depends on the training dataset, requires more work than just improving hyperparameters or adding extra components [5]. Future research should improve fraud detection performance by resolving class imbalances, incorporating additional ensemble models, and focusing on hyperparameter optimization. Strategies to ensure model adaptability to evolving fraud patterns and real-time data integration should be explored, improving system responsiveness. Future research should also focus on improving model interpretability to provide valuable insights into trust-building mechanisms and refine fraud detection techniques.

ACKNOWLEDGMENT

The authors would like to extend their gratitude to Khon Kaen University for their support through Announcement No. 2580/2563 on "The Criteria for the Acceptance of an Inbound Visiting Scholar from a Foreign Institution or Organization to Khon Kaen University." This support has been invaluable to the success of our research project.

REFERENCES

[1] N. I. Mustika, B. Nenda, and D. Ramadhan, "Machine Learning Algorithms in Fraud Detection: Case Study on Retail Consumer Financing Company," *Asia Pacific Fraud Journal*, vol. 6, no. 2, pp. 213–221, Dec. 2021, https://doi.org/10.21532/apfjournal.v6i2.216.

[2] K. Khando, M. S. Islam, and S. Gao, "The Emerging Technologies of Digital Payments and Associated Challenges: A Systematic Literature Review," *Future Internet*, vol. 15, no. 1, Jan. 2023, Art. no. 21, https://doi.org/10.3390/fi15010021.

[3] J. K. Afriyie *et al.*, "A supervised machine learning algorithm for detecting and predicting fraud in credit card transactions," *Decision Analytics Journal*, vol. 6, Mar. 2023, Art. no. 100163, https://doi.org/10.1016/j.dajour.2023.100163.

[4] S. Gold, "The evolution of payment card fraud," *Computer Fraud & Security*, vol. 2014, no. 3, pp. 12–17, Mar. 2014, https://doi.org/10.1016/S1361-3723(14)70471-3.

[5] H. Alizadeh and B. M. Bidgoli, "Introducing A Hybrid Data Mining Model to Evaluate Customer Loyalty," *Engineering, Technology & Applied Science Research*, vol. 6, no. 6, pp. 1235–1240, Dec. 2016, https://doi.org/10.48084/etasr.741.

[6] R. Y. R. Abdaljawad, T. Obaid, and S. S. Abu-Naser, "Fraudulent Financial Transactions Detection Using Machine Learning," in *2023 3rd International Conference on Emerging Smart Technologies and*

Applications (eSmarTA), Taiz, Yemen, Oct. 2023, https://doi.org/10.1109/eSmarTA59349.2023.10293697.

[7] T. C. Tran and T. K. Dang, "Machine Learning for Prediction of Imbalanced Data: Credit Fraud Detection," in *2021 15th International Conference on Ubiquitous Information Management and Communication (IMCOM)*, Seoul, Korea (South), Jan. 2021, pp. 1–7, https://doi.org/10.1109/IMCOM51814.2021.9377352.

[8] K. S. Lim, L. H. Lee, and Y. W. Sim, "A Review of Machine Learning Algorithms for Fraud Detection in Credit Card Transaction," *International Journal of Computer Science & Network Security*, vol. 21, no. 9, pp. 31–40, 2021, https://doi.org/10.22937/IJCSNS.2021.21.9.4.

[9] O. Kolodiziev, A. Mints, P. Sidelov, I. Pleskun, and O. Lozynska, "Automatic machine learning algorithms for fraud detection in digital payment systems," *Eastern-European Journal of Enterprise Technologies*, vol. 5, no. 9 (107), pp. 14–26, Oct. 2020, https://doi.org/10.15587/1729-4061.2020.212830.

[10] R. B. Sulaiman, V. Schetinin, and P. Sant, "Review of Machine Learning Approach on Credit Card Fraud Detection," *Human-Centric Intelligent Systems*, vol. 2, no. 1, pp. 55–68, Jun. 2022, https://doi.org/10.1007/s44230-022-00004-0.

[11] P. K. Sadineni, "Detection of Fraudulent Transactions in Credit Card using Machine Learning Algorithms," in *2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)*, Palladam, India, Oct. 2020, pp. 659–660, https://doi.org/10.1109/I-SMAC49090.2020.9243545.

[12] V. N. Dornadula and S. Geetha, "Credit Card Fraud Detection using Machine Learning Algorithms," *Procedia Computer Science*, vol. 165, pp. 631–641, Jan. 2019, https://doi.org/10.1016/j.procs.2020.01.057.

[13] N. Baisholan, M. Turdalyuly, S. Gnatyuk, and K. Kubayev, "Implementation of Machine Learning Techniques To Detect Fraudulent Credit Card Transactions on a Designed Dataset," *Journal of Theoretical and Applied Information Technology (JATIT)*, vol. 101, no. 13, pp. 5279–5287, Jul. 2023.

[14] V. Plotnikova, M. Dumas, and F. P. Milani, "Applying the CRISP-DM data mining process in the financial services industry: Elicitation of adaptation requirements," *Data & Knowledge Engineering*, vol. 139, May 2022, Art. no. 102013, https://doi.org/10.1016/j.datak.2022.102013.

[15] C. El Morr, M. Jammal, H. Ali-Hassan, and W. EI-Hallak, *Machine Learning for Practical Decision Making: A Multidisciplinary Perspective with Applications from Healthcare, Engineering and Business Analytics*, vol. 334. Cham, Switzerland: Springer International Publishing, 2022, https://doi.org/10.1007/978-3-031-16990-8.

[16] N. Axford, "Logistic regression," in *Exploring Concepts of Child Well-Being: Implications for Children's Services*. Bristol, UK: Policy Press, 2008, pp. 209–212.

[17] M. Loukili, F. Messaoudi, and M. El Ghazi, "Machine learning based recommender system for e-commerce," *IAES International Journal of Artificial Intelligence (IJ-AI)*, vol. 12, no. 4, pp. 1803–1811, Dec. 2023, https://doi.org/10.11591/ijai.v12.i4.pp1803-1811.

[18] T. Andi and E. Utami, "Association rule algorithm with FP growth for book search," in *IOP Conference Series: Materials Science and Engineering*, Bandung, Indonesia, Apr. 2018, vol. 434, https://doi.org/10.1088/1757-899X/434/1/012035.

[19] P. Cunningham and S. J. Delany, "k-Nearest Neighbour Classifiers - A Tutorial," *ACM Computing Surveys*, vol. 54, no. 6, pp. 1–25, Jul. 2021, Art. no. 128, https://doi.org/10.1145/3459665.

[20] E. Altman, A. Nitsure, and Y. Mroueh, “Credit Card Transactions.” Kaggle, [Online]. Available: https://www.kaggle.com/datasets/ealtman2019/credit-card-transactions.

[21] N. Rtayli and N. Enneya, "Enhanced credit card fraud detection based on SVM-recursive feature elimination and hyper-parameters optimization," *Journal of Information Security and Applications*, vol. 55, Dec. 2020, Art. no. 102596, https://doi.org/10.1016/j.jisa.2020.102596.

[22] A. Hemmati, H. Nasiri, M. A. Haeri, and M. M. Ebadzadeh, "A Novel Correlation-Based CUR Matrix Decomposition Method," in *2020 6th International Conference on Web Research (ICWR)*, Tehran, Iran, Apr. 2020, pp. 172–176, https://doi.org/10.1109/ICWR49608.2020.9122286.

[23] D. S. Sisodia, N. K. Reddy, and S. Bhandari, "Performance evaluation of class balancing techniques for credit card fraud detection," in *2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI)*, Chennai, India, Sep. 2017, pp. 2747–2752, https://doi.org/10.1109/ICPCSI.2017.8392219.

[24] E. Ileberi, Y. Sun, and Z. Wang, "A machine learning based credit card fraud detection using the GA algorithm for feature selection," *Journal of Big Data*, vol. 9, no. 1, pp. 1–17, Feb. 2022, Art. no. 24, https://doi.org/10.1186/s40537-022-00573-8.

[25] J. L. Speiser, M. E. Miller, J. Tooze, and E. Ip, "A comparison of random forest variable selection methods for classification prediction modeling," *Expert Systems with Applications*, vol. 134, pp. 93–101, Nov. 2019, https://doi.org/10.1016/j.eswa.2019.05.028.

[26] S. Xuan, G. Liu, Z. Li, L. Zheng, S. Wang, and C. Jiang, "Random forest for credit card fraud detection," in *2018 IEEE 15th International Conference on Networking, Sensing and Control (ICNSC)*, Zhuhai, China, Mar. 2018, pp. 1–6, https://doi.org/10.1109/ICNSC.2018.8361343.

[27] J. V. S. Gollapalli, S. Kalambele, A. Jain, and E. Ariwa, "Emerging Trends of AI and Digital Transactions Replacing Plastic Money in India," in *The Business of the Metaverse*, 1st ed. New York, NY, USA: Productivity Press, 2023.