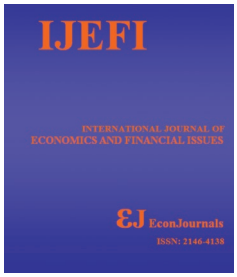


International Journal of Economics and Financial Issues

ISSN: 2146-4138

available at http: www.econjournals.com

International Journal of Economics and Financial Issues, 2024, 14(5), 177-184.

Enhancing Fraud Detection in Banking using Advanced Machine Learning Techniques

Umawadee Detthamrong[1], Wirapong Chansanam[2]*, Tossapon Boongoen[3], Natthakan Iam-On[3]

[1]College of Local Administration, Khon Kaen University, Khon Kaen, Thailand, [2]Faculty of Humanities and Social Sciences, Khon Kaen University, Khon Kaen, Thailand, [3]Department of Computer Science, Aberystwyth University, Aberystwyth, United Kingdom, *Email: wirach@kku.ac.th

Received: 01 April 2024 **Accepted:** 19 July 2024 **DOI:** https://doi.org/10.32479/ijefi.16613

ABSTRACT

This study demonstrates the effectiveness of advanced machine learning techniques in detecting fraudulent activities within the banking industry. We evaluated the performance of various models, including LightGBM, XGBoost, CatBoost, vote classifiers, and neural networks, on a comprehensive dataset of banking transactions. The CatBoost model exhibited the highest accuracy in identifying fraudulent instances, showcasing its superior performance. The application of diverse sampling and scaling techniques significantly improved fraud detection accuracy, emphasizing their crucial role in the process. Furthermore, the incorporation of the CatBoost ensemble method substantially enhanced the efficiency of fraud identification. Our findings underscore the potential of these advanced machine-learning approaches in mitigating financial losses and ensuring secure transactions, ultimately bolstering trust and security in the banking sector. Future research directions include refining the CatBoost model's hyper parameters, adapting to evolving fraud patterns, and integrating real-time data for enhanced responsiveness. Additionally, efforts will be made to improve the interpretability of the model's decision-making process, providing valuable insights into its trust-building capabilities and enhancing the transparency of fraud detection methodologies.

Keywords: Fraud Detection, Machine Learning, CatBoost, Banking Security, Ensemble Methods
JEL Classifications: G2, G4, G5

1. INTRODUCTION

In the era of rapid digital transformation, the banking industry faces an unprecedented challenge in combating fraudulent activities. As online transactions and digital payment methods continue gaining popularity, financial fraud has risen dramatically, resulting in substantial economic losses for customers and financial institutions (Ghai and Kang, 2021). The sophistication and diversity of fraudulent techniques, such as phishing scams, malware infections, and ghost websites, have rendered traditional rule-based fraud detection approaches increasingly ineffective (Minastireanu and Mesnita, 2019).

To address this pressing issue, researchers and industry experts have turned to advanced machine learning techniques, harnessing the power of data mining and artificial intelligence to develop more robust and adaptive fraud detection systems. These cutting-edge approaches have the potential to learn from vast amounts of transaction data, uncover complex patterns, and adapt to the ever-evolving tactics employed by fraudsters (Manikandaprabhu et al., 2023). By leveraging machine learning algorithms, financial institutions can significantly enhance the accuracy and efficiency of their fraud detection processes, ultimately protecting their customers and maintaining trust in the financial system.

The previous research explored the application of state-of-the-art machine learning techniques in enhancing fraud detection within the banking sector. By examining various approaches, such as deep learning, anomaly detection, clustering techniques, and multi-layer models, they seek to identify the most effective methods for accurately classifying fraudulent transactions while minimizing false

positives (Banerjee et al., 2018; Marchal and Szyller, 2019; Nanduri et al., 2020; Roy et al., 2018). Furthermore, they delved into the unique challenges posed by different types of fraud, including credit card fraud, online banking fraud, and first-party fraud, discussed the limitations of existing detection systems and the advantages of employing machine learning solutions (Krishna et al., 2023; Amasiatu and Shah, 2018; Wickramanayake et al., 2020).

The impact of financial fraud extends beyond the immediate monetary losses, as it can erode customer trust and hinder the growth of the digital economy. Timely detection is crucial, as the chances of recovering losses diminish significantly if fraud is not identified promptly (Minastireanu and Mesnita, 2019). However, the dynamic nature of fraudulent activities and the resemblance of fraudulent transactions to legitimate ones pose significant challenges to existing fraud detection techniques (Kemp, 2020). Therefore, there is a pressing need for innovative approaches that can adapt to the evolving fraud landscape and provide accurate, real-time detection (Amanze et al., 2018).

This paper aims to provide valuable insights for the banking industry, financial institutions, and academicians by conducting a comprehensive review and investigate of the current research landscape and proposing novel approaches. In fraud detection, we will explore the strengths and weaknesses of various machine learning algorithms, such as neural networks, decision trees, support vector machines, K-nearest neighbor, logistic regression, random forest, and naïve Bayes (Shin and Lee, 2002; Maher, 2020). Additionally, we will discuss the importance of feature engineering techniques for behavioral profiling and the need for adaptive efforts to address the evolving nature of fraud (Wickramanayake et al., 2020).

Through this research, we aim to empower financial institutions to refine their fraud detection strategies, leveraging the latest advancements in machine learning to combat this pervasive threat effectively. By providing a roadmap for implementing advanced fraud detection systems, we hope to contribute to developing a more secure and trustworthy financial ecosystem, fostering the growth of the digital economy while protecting the interests of customers and businesses alike.

2. METHODOLOGY

This research develops an advanced approach for detecting fraudulent activities in banking data using machine learning techniques. The method's effectiveness is enhanced through the application of Bayesian optimization and class weight-tuning, as well as the utilization of algorithms such as CatBoost, LightGBM, and XGBoost (Jabeur et al., 2021; Hancock and Khoshgoftaar, 2020; Chen and Han, 2021; Dhananjay and Sivaraman, 2021). The incorporation of deep learning further improves the system's performance. Rigorous testing using real-world data and key metrics has been conducted to ensure the system's efficacy in detecting and preventing fraudulent transactions. The proposed approach includes a Stacking Classifier that combines the predictions of the Random Forest and LightGBM (Taha and Malebary, 2020; Liang et al., 2020) classifiers with specific configurations. This ensemble method enhances the accuracy of predictions by leveraging the strengths of different models, with a Gradient Boosting Classifier serving as the final predictor.

The system's input consists of raw data about credit card transactions, including labels and features indicating whether a transaction is legitimate or fraudulent. Preprocessing, which involves feature selection and extraction, is required to prepare the data for machine learning. The dataset is divided into two subsets: a training set for model development and a test set for evaluating model performance. Bayesian optimization is employed to optimize the hyperparameters of the machine learning algorithms. Five-fold cross-validation is applied to machine learning algorithms such as CatBoost, LightGBM (Alothman et al., 2022; Taha and Malebary, 2020), and XGBoost on the training data to ensure model robustness. We have also explored the stacked algorithm as an extension to the project. Multiple evaluation metrics are utilized to assess the models' performance in detecting credit card fraud while minimizing false positives.

The machine learning models in this study were trained using the Credit Card Fraud Detection dataset obtained from Kaggle. The original dataset contained various attributes associated with credit card transactions, including "Amount," "Time," and features labeled "V1" through "V28." To maintain confidentiality, sensitive information and details about the original features were anonymized. The dataset used in this research can be accessed through the following Kaggle link: https://www.kaggle.com/datasets/arockiaselciaa/creditcardcsv. Researchers and practitioners interested in replicating or building upon this work can obtain the necessary data from the provided source. To streamline the comparative study and evaluate algorithms that align with enhancing fraud detection in banking, we provided code examples at the beginning of each Python script on our system's web page hosted on Google Colab. The code repository can be accessed at the following URL: https://colab.research.google.com/drive/1B-l25t2VyFesL8ye2e1UPfmR5CMpHpVC?usp=sharing. This allows for easy replication and comparison of the algorithms' performance in detecting fraudulent activities within the banking sector.

Figure 1 illustrates the descriptive statistics for each parameter, including the count, mean, standard deviation (SD), minimum, and maximum values. The count represents the total number of observations for each parameter. The mean provides the average value, while the standard deviation (SD) indicates the amount of variation or dispersion from the mean. The minimum and maximum values reflect the smallest and largest observations, respectively, within each parameter's dataset. This comprehensive summary offers a clear overview of the central tendency and variability present in the data. Figure 1 provides a concise overview of the dataset's characteristics. It allows researchers and analysts to quickly assess the central tendency, variability, and range of each parameter. This information is essential for understanding the nature of the data, identifying potential anomalies, and making informed decisions about further analysis or modeling techniques.

Figure 2 provides a clear visual representation of the proportion of valid and fraudulent transactions. The pie chart divides the

Figure 1: Histograms of individual parameter

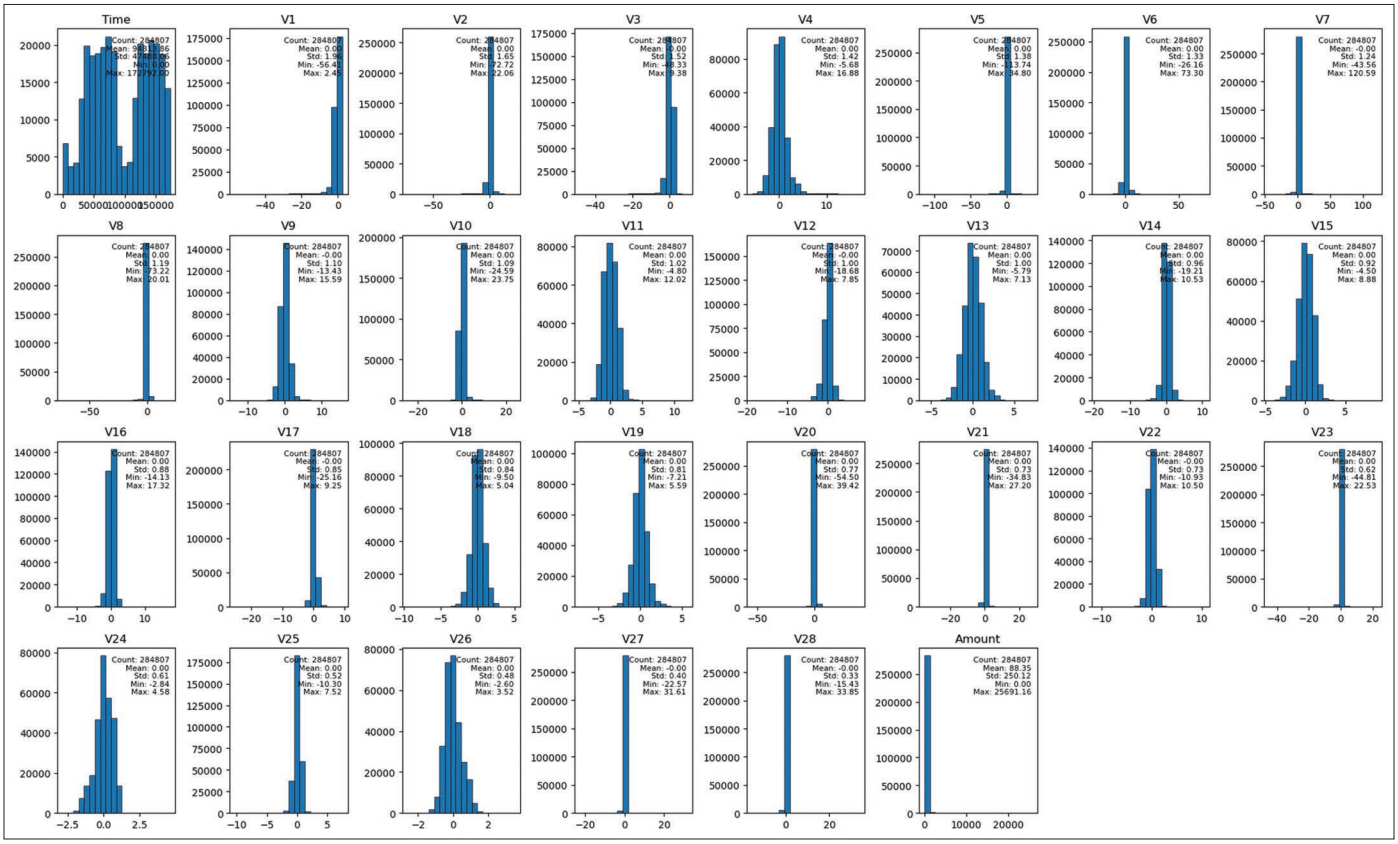


Figure 2: Pie Chart for number and percentage of fraudulent versus valid transactions

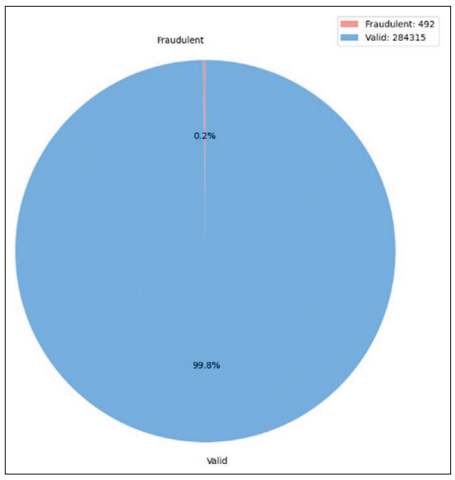
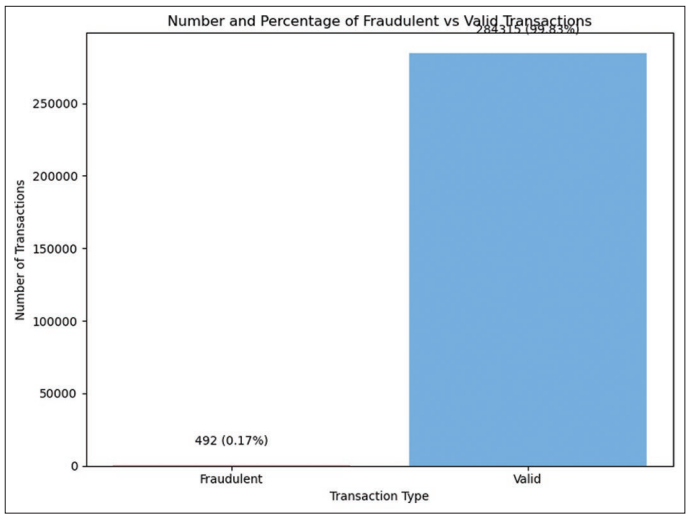


Figure 3: Plot for number and percentage of fraudulent versus valid transactions



total number of transactions into two segments: one for valid transactions and the other for fraudulent ones. Each segment of the chart is labeled with both the number and percentage of transactions it represents, making it easy to understand the relative frequency of fraudulent activities compared to legitimate ones. This visual aid simplifies the interpretation of data, highlighting the extent of fraudulent transactions within the dataset, which is crucial for identifying the need for enhanced security measures and strategies to mitigate fraud.

Figure 3 offers a clear and informative graphical representation of the number and percentage of fraudulent and valid transactions in the dataset. By combining visual and numerical information, the plot provides a comprehensive and easily interpretable overview of the data, facilitating understanding and communication of the findings. The inclusion of precise values and percentages enhances the accuracy and transparency of the data presentation, making it a valuable tool for conveying the distribution of transaction types in the dataset.

2.1. Data Processing

Data processing is crucial to converting raw, unstructured data into actionable insights for businesses. This process typically

involves data scientists engaging in various steps, including data collection, organization, cleaning, validation, analysis, and transformation into readable formats such as graphs or reports. Data processing can be categorized into three main approaches: manual, mechanical, or electronic. The primary objective of data processing is to enhance the usability of information and facilitate decision-making processes. By streamlining data processing, companies can improve their operational efficiency and rapidly make informed strategic decisions. Automated data processing tools, such as computer software, play a significant role in enabling this process. These tools can effectively transform large datasets and other data types into valuable information for decision-making and quality control.

2.2. Feature Selection

Feature selection is a critical step in the model development process, which involves identifying the most reliable, informative, and non-redundant attributes to construct a model. As the volume and variety of records continue to grow, it becomes increasingly important to reduce their dimensionality systematically. One of the primary objectives of feature selection is to enhance a model's predictive performance while minimizing computational complexity.

Feature selection is a key component of feature engineering, which is selecting the most relevant features to input into machine learning algorithms. Feature selection techniques eliminate irrelevant or redundant features, retaining only the most significant ones for the machine learning model. This process reduces the number of input variables. Several significant benefits can be achieved by preselecting the most important features instead of relying on the machine learning model to perform this task.

2.3. Algorithms

2.3.1. Light gradient boosting machine (LGBM)

LGBM is a highly efficient gradient boosting framework that excels in handling large datasets with remarkable speed. It is renowned for its fast performance and high accuracy, making it suitable for tasks such as fraud detection. LGBM constructs an ensemble of decision trees and optimizes the boosting process to achieve faster convergence of results (Liang et al., 2020).

$$\text{Objective function} = \Sigma(i=1 \text{ to } n)\ \text{loss}(y\_i, \hat{y}\_i) + \alpha * \Sigma(j=1 \text{ to } m)\ |w\_j| + \lambda * \Sigma(j=1 \text{ to } m)\ w\_j^2$$

where:

- n is the number of training instances
- y_i is the actual target value for instance i
- ŷ_i is the predicted value for instance i
- m is the number of model parameters (weights)
- w_j is the weight of parameter j
- α is the L1 regularization parameter
- λ is the L2 regularization parameter

2.3.2. Extreme gradient boosting (XGBoost)

XGBoost is another widely used gradient boosting method for machine learning tasks. It is known for its robustness and excellent performance. XGBoost effectively handles imbalanced datasets by employing a regularized gradient boosting scheme, which is crucial for fraud detection.

$$\text{Objective function} = \Sigma(i=1 \text{ to } n)\ \text{loss}(y\_i, \hat{y}\_i) + \Omega(f)$$

where:

- n is the number of training instances
- y_i is the actual target value for instance i
- ŷ_i is the predicted value for instance i
- Ω(f) is the regularization term

The regularization term Ω(f) is defined as:

$$\Omega(f) = \gamma * T + 0.5 * \lambda * \Sigma(j=1 \text{ to } T)\ w\_j^2$$

where:

- γ is the complexity parameter for the number of leaves
- T is the number of leaves in the tree
- λ is the L2 regularization parameter
- w_j is the weight (score) of leaf j

XGBoost also employs techniques such as column subsampling, row subsampling, and shrinkage (learning rate) to further improve the model's generalization ability and prevent overfitting.

The algorithm iteratively adds new trees to the ensemble, with each tree being trained on the residuals (errors) of the previous trees. This process continues until a stopping criterion is met, such as reaching a maximum number of iterations or achieving a satisfactory level of performance.

2.3.3. Categorical boosting (CatBoost)

CatBoost is a gradient boosting library designed to handle categorical features effectively. It automatically processes categorical data, making it user-friendly. CatBoost is less prone to overfitting and can be beneficial when working with real-world banking data (Jabeur et al., 2021; Hancock and Khoshgoftaar, 2020; Chen and Han, 2021; Dhananjay and Sivaraman, 2021).

$$\text{Objective function} = \Sigma(i=1 \text{ to } n)\ \text{loss}(y\_i, \hat{y}\_i) + \lambda * \Sigma(j=1 \text{ to } m)\ w\_j^2 + \gamma * \Phi(T)$$

where:

- n is the number of training instances
- y_i is the actual target value for instance i
- ŷ_i is the predicted value for instance i
- m is the number of model parameters (weights)
- w_j is the weight of parameter j
- λ is the L2 regularization parameter
- γ is the model complexity regularization parameter
- Φ(T) is a function that measures the complexity of the decision trees based on the number of splits and the depth of the trees

2.3.4. Logistic regression

Logistic Regression is one of the most fundamental binomial classification algorithms. Although it may not be as sophisticated as ensemble methods like boosting, it can serve as a baseline for fraud detection. Its simplicity and interpretability can provide

insights into feature importance. In mathematical notation, the logistic regression formula can be represented as:

$$P(y = 1 \mid x) = 1/(1 + e^{(-z)})$$

where:

- $P(y = 1 \mid x)$ is the probability of the positive class given the input features x
- y is the binary class label (1 for the positive class, 0 for the negative class)
- x is the vector of input feature values
- z is the linear combination of the input features and their corresponding weights, plus the bias term

The logistic regression model can be extended to handle multi-class classification problems by using techniques such as one-versus-rest (OvR) or softmax regression. In these cases, separate logistic regression models are trained for each class, and the final prediction is made based on the class with the highest predicted probability.

Overall, logistic regression is a simple yet powerful algorithm for binary classification tasks, providing a probabilistic interpretation of the predictions and allowing for easy understanding of the impact of each input feature on the outcome.

2.4. Voting Classifier

The Voting Classifier combines predictions from multiple machine learning models, such as Logistic Regression, XGBoost, and CatBoost, to generate a final prediction. This ensemble method leverages the collective knowledge of different models, often resulting in improved accuracy and robustness. We have constructed several voting models utilizing various combinations of algorithms (Vairam et al., 2022; Rakhshaninejad et al., 2022).

2.5. Neural Network

A Neural Network is a deep learning model inspired by the functioning of the human brain. In this context, it can capture complex patterns and relationships within the data. Neural networks are employed for their ability to learn intricate fraud patterns, particularly in large datasets.

2.6. Stacking Classifier

As an extension, we have developed a stacking classifier.

The Stacking Classifier is an ensemble method that combines predictions from two base classifiers (Random Forest and LightGBM) with specific configurations. It utilizes a Gradient Boosting Classifier as the final predictor to enhance the accuracy of predictions by leveraging the strengths of different models in ensemble learning.

3. EXPERIMENTAL RESULTS

3.1. Precision

Precision is a metric that measures the proportion of correctly classified instances or samples among those predicted as positive cases. It quantifies the accuracy of positive predictions made by the model. The formula to calculate precision is as follows:

$$\text{Precision} = \text{True Positives}/(\text{True Positives} + \text{False Positives})$$

3.2. Recall

In the context of machine learning, recall is a metric that indicates the ability of a model to identify all the relevant instances of a particular class. It measures the model's effectiveness in capturing the true positive cases. Recall is calculated by dividing the number of correctly predicted positive instances by the total number of actual positive instances in the dataset.

$$\text{Recall} = \text{True Positives}/(\text{True Positives}+\text{False Negatives})$$

3.3. Accuracy

Accuracy is a commonly used metric that represents the overall correctness of a classification model's predictions. It is calculated as the ratio of correctly classified instances to the total number of instances in the dataset.

$$\text{Accuracy} = (\text{True Positives}+\text{True Negatives})/(\text{True Positives}+\text{True Negatives}+\text{False Positives}+\text{False Negatives})$$

3.4. F1 Score

The F1 score is the harmonic mean of precision and recall, providing a balanced measure that takes into account both false positives and false negatives. It is particularly useful when dealing with imbalanced datasets, as it considers both the model's ability to correctly identify positive instances and its ability to avoid false positives.

$$\text{F1 Score} = 2 \times (\text{Precision} \times \text{Recall})/(\text{Precision} + \text{Recall})$$

The F1 score ranges from 0 to 1, with higher values indicating better performance. It strikes a balance between precision and recall, making it a comprehensive evaluation metric for classification tasks.

These metrics provide valuable insights into the performance of a machine learning model. Precision focuses on the correctness of positive predictions, while recall measures the model's ability to capture all the relevant instances. Accuracy provides an overall assessment of the model's correctness, while the F1 score combines precision and recall to offer a balanced evaluation, especially in the presence of class imbalance.

By calculating and analyzing these metrics, researchers and practitioners can gain a deeper understanding of a model's strengths and weaknesses, and make informed decisions about model selection, optimization, and deployment in real-world applications.

Table 1 presents the performance evaluation of various machine learning models for a classification task. The models evaluated include CatBoost, LightGBM, XGBoost, Logistic Regression, Voting Classifier, Neural Network, and Stacking Classifier. The performance metrics used for evaluation are Accuracy, Precision, Recall, F1 Score, and ROC AUC.

Table 1: Performance evaluation table

Metric	CatBoost	LightGBM	XGBoost	Logistic Regression	Voting Classifier	Neural Network	Stacking Classifier
Accuracy	0.999648889	0.997349110	0.999561111	0.967434430	0.999596222	0.997700221	0.999596222
Precision	0.975609756	0.291338583	0.962025316	0.046931408	0.974683544	0.413612565	0.974683544
Recall	0.816326531	0.377551020	0.775510204	0.928571429	0.785714286	0.806122449	0.785714286
F1 Score	0.888888889	0.328888889	0.858757062	0.089347079	0.870056497	0.546712803	0.870056497
ROC AUC	0.908145679	0.687984148	0.887728723	0.948036418	0.892839557	0.902076419	0.892839557

Among the models, CatBoost achieves the highest accuracy of 0.999648889, indicating its excellent ability to correctly classify instances. It also demonstrates strong performance in terms of Precision (0.975609756), Recall (0.816326531), F1 Score (0.888888889), and ROC AUC (0.908145679).

The Stacking Classifier and Voting Classifier also exhibit impressive performance, with high accuracy scores of 0.999596222 and similar values for Precision, Recall, and F1 Score. The Neural Network model follows closely, with an accuracy of 0.997700221 and competitive scores in other metrics.

XGBoost and LightGBM show slightly lower accuracy compared to CatBoost but still achieve good performance overall. XGBoost has a higher Precision (0.962025316) and F1 Score (0.858757062) compared to LightGBM, while LightGBM has a better Recall (0.377551020).

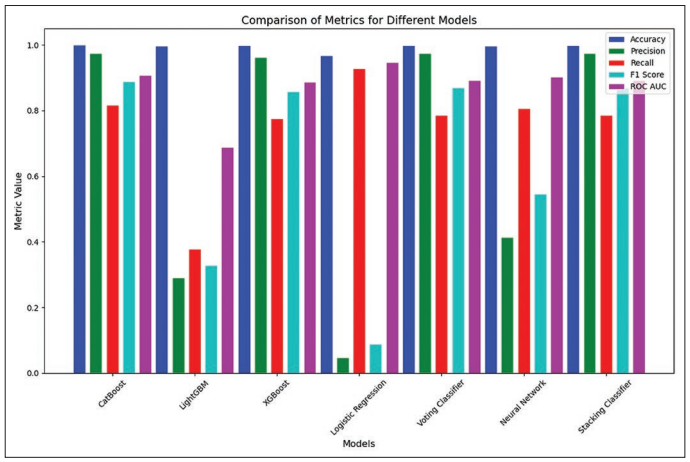
Logistic Regression, despite its simplicity, demonstrates a high Recall of 0.928571429, indicating its ability to identify positive instances. However, it has lower scores in Precision (0.046931408) and F1 Score (0.089347079) compared to other models.

The ROC AUC metric, which measures the overall discrimination ability of the models, shows that all models perform well, with scores ranging from 0.687984148 (LightGBM) to 0.948036418 (Logistic Regression).

In summary, CatBoost emerges as the top-performing model across most metrics, followed closely by the Stacking Classifier, Voting Classifier, and Neural Network. XGBoost and LightGBM also provide competitive results, while Logistic Regression excels in Recall but lags in other metrics. The choice of the best model depends on the specific requirements of the classification task and the trade-offs between different performance metrics.

Figure 4 presents a comprehensive comparison of the performance of various algorithms using key evaluation metrics: precision, Matthews Correlation Coefficient (MCC), F1 score, and recall. This visual representation allows for a clear differentiation between the algorithms based on their effectiveness in the given task. By providing this differentiation between algorithms using multiple evaluation metrics, Figure 4 offers a comprehensive overview of their performance. It enables readers to assess the strengths and weaknesses of each algorithm in terms of precision, MCC, F1 score, and recall. This information is crucial for making informed decisions about algorithm selection, as different metrics may be more important depending on the specific requirements of the task at hand.

Figure 4: Comparison bar graph between previous and obtained value



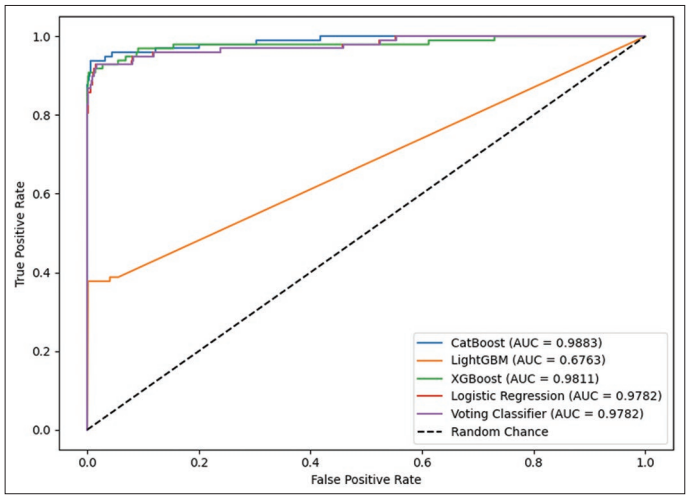
Furthermore, Figure 4 may include additional visual elements, such as color-coding or highlighting, to emphasize the best-performing algorithms for each metric. Figure 4 provides a valuable visual comparison of the performance of different algorithms using precision, MCC, F1 score, and recall. It allows readers to differentiate between the algorithms based on their effectiveness in the given task and make informed decisions about algorithm selection. The visual representation enhances the understanding of the algorithms' strengths and weaknesses, facilitating a comprehensive evaluation of their performance.

Figure 5 shows the Receiver Operating Characteristic (ROC) curves for each model, illustrating their performance in binary classification. The ROC curve plots the True Positive Rate (TPR) against the False Positive Rate (FPR) at various thresholds, indicating each model's ability to correctly identify positive instances (TPR) while minimizing false alarms (FPR). An ideal model's curve hugs the top-left corner, reflecting high TPR and low FPR. The diagonal line represents random classification, and models above this line perform better than random. The Area Under the Curve (AUC) value, included in Figure 5, quantifies overall model performance.

4. DISCUSSION

In this study, we evaluated the performance of various machine learning models for fraud detection in the banking industry. CatBoost demonstrated superior accuracy among the models tested, showcasing its effectiveness in identifying fraudulent activities (Ibrahim et al., 2020; Huang and Yen, 2019). The project's robust results across multiple machine learning models, including LightGBM, XGBoost, CatBoost (Özlem and Tan, 2022; Jabeur et al., 2021; Hancock and Khoshgoftaar, 2020; Chen and Han, 2021; Dhananjay and Sivaraman, 2021), voting

Figure 5: Plot for the receiver operating characteristic curve and area under the curve



classifiers, and neural networks, highlight the versatility of the approach. The application of diverse sampling and scaling techniques significantly enhanced the accuracy of fraud detection, emphasizing the importance of these preprocessing methods. Furthermore, utilizing the CatBoost ensemble method greatly improved the efficiency of fraud identification, demonstrating its effectiveness (Adane et al., 2023; Yang et al., 2023; Yanuar et al., 2023; Nguyen et al., 2022; Postalcioglu, 2022; Ogar et al., 2022; Nanduri et al., 2020; Matloob et al., 2022; Feng, 2021).

The findings of this research underscore the potential of advanced machine learning techniques in detecting fraudulent activities within the banking sector, paving the way for further applications and improvements. The results allow continued enhancements by exploring additional ensemble methods and optimization strategies. Ultimately, the research's outcomes contribute to the banking industry by facilitating more effective fraud detection, reducing financial losses, and ensuring the security of transactions, thereby enhancing overall trust and security.

Future research directions will focus on improving the accuracy and robustness of fraud detection by incorporating more hybrid models with CatBoost (Jabeur et al., 2021). Fine-tuning of CatBoost's hyperparameters will be explored, specifically determining the optimal number of trees to enhance model performance (Goyal and Khiari, 2020). Efforts will be made to ensure the model's adaptability to evolving fraud patterns, enabling it to detect emerging fraudulent activities continuously. The real-time data integration will be a key focus of ongoing research, aiming to increase the model's responsiveness and adaptability, allowing for swift reactions to new threats. Future work will also focus on enhancing the interpretability of the model's decision-making process, providing deeper insights into its functionality, and improving the transparency of fraud detection techniques.

5. CONCLUSION

This study comprehensively evaluated various machine learning models for fraud detection in banking, demonstrating the superior accuracy of the CatBoost model in identifying fraudulent activities. The robust outcomes across multiple models like LightGBM, XGBoost, voting classifiers, and neural networks highlight the versatility of the approach. Applying diverse sampling and scaling techniques significantly boosted fraud detection accuracy, emphasizing the importance of preprocessing and utilizing the CatBoost ensemble method, which substantially improved fraud identification efficiency, solidifying its effectiveness.

The findings accentuate the immense potential of advanced machine-learning techniques for banking fraud detection. The results pave the way for further enhancements by exploring additional ensemble methods and optimization strategies to augment model accuracy and robustness. Crucially, the research contributes to more effective fraud detection, reducing financial losses and ensuring secure transactions, fostering heightened trust and security for institutions and customers.

Future efforts will focus on incorporating more CatBoost hybrid models, fine-tuning hyperparameters like optimal tree numbers to boost performance, ensuring model adaptability to evolving fraud patterns for continuous detection, integrating real-time data for responsiveness, and enhancing interpretability of decision-making processes. This study significantly advances fraud detection through machine learning applications, laying the foundation for continued innovation in this critical domain.

6. ACKNOWLEDGMENTS

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

Adane, K., Beyene, B., Abebe, M. (2023), Single and hybrid-ensemble learning-based phishing website detection: Examining impacts of varied nature datasets and informative feature selection technique. Digital Threats: Research and Practice, 4(3), 1-27.

Alothman, R., AliTalib, H., Mohammed, M.S. (2022), Fraud detection under the unbalanced class based on gradient boosting. Eastern-European Journal of Enterprise Technologies, 116(2), 254922.

Amanze, B.C., Inyiama, H.C., Onyesolu, M.O. (2018), On the development of credit card fraud detection system using multi-agents. International Journal on Computer Science and Engineering, 6(6), 1333-1343.

Amasiatu, C.V., Shah, M.H. (2018), First party fraud management: Framework for the retail industry. International Journal of Retail and Distribution Management, 46, 350-363.

Banerjee, R., Bourla, G., Chen, S., Kashyap, M., Purohit, S. (2018), Comparative Analysis of Machine Learning Algorithms through Credit Card Fraud Detection. In: 2018 IEEE MIT Undergraduate Research Technology Conference (URTC). p1-4.

Chen, Y., Han, X. (2021), CatBoost for Fraud Detection in Financial Transactions. In: Proceedings of the IEEE International Conference on Consumer Electronics and Computer Engineering (ICCECE).

p176-179.
Dhananjay, B., Sivaraman, J. (2021), Analysis and classification of heart rate using CatBoost feature ranking model. Biomedical Signal Processing and Control, 68, 102610.
Feng, H. (2021), Ensemble Learning in Credit Card Fraud Detection using Boosting Methods. In: Proceedings of the 2nd International Conference on Computer and Data Science (CDS). p7-11.
Ghai, V., Kang, S.S. (2021), Role of Machine Learning in Credit Card Fraud Detection. In: 2021 3rd International Conference on Advances in Computing, Communication Control and Networking (ICAC3N). IEEE. p939-943.
Goyal, A., Khiari, J. (2020), Diversity-Aware Weighted Majority Vote Classifier for Imbalanced Data. In: Proceedings of the International Joint Conference on Neural Networks (IJCNN). p1-8.
Hancock, J., Khoshgoftaar, T.M. (2020), Medicare Fraud Detection Using CatBoost. In: Proceedings of the IEEE 21st International Conference on Information Reuse and Integration for Data Science (IRI). p97-103.
Huang, Y.P., Yen, M.F. (2019), A new perspective of performance comparison among machine learning algorithms for financial distress prediction. Applied Soft Computing, 83, 105663.
Ibrahim, A.A., Ridwan, R.L., Muhammed, M.M., Abdulaziz, R.O., Saheed, G.A. (2020), Comparison of the CatBoost classifier with other machine learning methods. International Journal of Advanced Computer Science and Applications, 11(11), 0111190.
Jabeur, S.B., Gharib, C., Mefteh-Wali, S., Arfi, W.B. (2021), CatBoost model and artificial intelligence techniques for corporate failure prediction. Technological Forecasting and Social Change, 166, 120658.
Kemp, S. (2020), Fraud reporting in Catalonia in the Internet era: Determinants and motives. European Journal of Criminology, 19, 994-1015.
Krishna, K.G., Kulkarni, P., Natraj, N.A. (2023), Use of Big Data Technologies for Credit Card Fraud Prediction. In: 2023 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS). p1408-1413.
Liang, W., Luo, S., Zhao, G., Wu, H. (2020), Predicting hard rock pillar stability using GBDT, XGBoost, and LightGBM algorithms. Mathematics, 8(5), 765.
Maher, P.E. (2020), The Seven Most Popular Machine Learning Algorithms for Online Fraud Detection and their Use in SAS®. Available from: https://communities.sas.com/t5/SAS-Communities-Library/The-seven-most-popular-machine-learning-algorithms-for-online/ta-p/668072
Manikandaprabhu, P., Prasanna, S., Sivaranjan, K., Senthilkumar, R. (2023), Fraudulent banking transaction classification using deep learning algorithm. International Journal of Advanced Research in Science, Communication and Technology, 3(1), 68-74.
Marchal, S., Szyller, S. (2019), Detecting Organized eCommerce Fraud using Scalable Categorical Clustering. In: Proceedings of the 35th Annual Computer Security Applications Conference. p215-228.
Matloob, I., Khan, S.A., Rukaiya, R., Khattak, M.A.K., Munir, A. (2022), A sequence mining-based novel architecture for detecting fraudulent transactions in healthcare systems. IEEE Access, 10, 48447-48463.
Minastireanu, E.A., Mesnita, G. (2019), An analysis of the most used machine learning algorithms for online fraud detection. Informatica Economica, 23(1), 5-16.
Nanduri, J., Liu, Y.W., Yang, K., Jia, Y. (2020), Ecommerce Fraud Detection through Fraud Islands and Multi-Layer Machine Learning Model. In: Proceedings of the Future Information and Communication Conference, Advances in Information and Communication. San Francisco, CA, USA: Springer. p556-570.
Nguyen, N., Duong, T., Chau, T., Nguyen, V.H., Trinh, T., Tran, D., Ho, T. (2022), A proposed model for card fraud detection based on Catboost and deep neural network. IEEE Access, 10, 96852-96861.
Ogar, V.N., Hussain, S., Gamage, K.A. (2022), Transmission line fault classification of multi-dataset using catboost classifier. Signals, 3(3), 468-482.
Özlem, Ş., Tan, O.F. (2022), Predicting cash holdings using supervised machine learning algorithms. Financial Innovation, 8(1), 44.
Postalcioglu, S. (2022), Design of automatic tool for diagnosis of pneumonia using boosting techniques. Brazilian Archives of Biology and Technology, 65, e22210322.
Rakhshaninejad, M., Fathian, M., Amiri, B., Yazdanjue, N. (2022), An ensemble-based credit card fraud detection algorithm using an efficient voting strategy. The Computer Journal, 65(8), 1998-2015.
Roy, A., Sun, J., Mahoney, R., Alonzi, L., Adams, S., Beling, P. (2018), Deep Learning Detecting Fraud in Credit Card Transactions. In: 2018 Systems and Information Engineering Design Symposium (SIEDS). p129-134.
Shin, K.S., Lee, Y.J. (2002), A genetic algorithm application in bankruptcy prediction modeling. Expert Systems with Applications, 23(3), 321-328.
Taha, A.A., Malebary, S.J. (2020), An intelligent approach to credit card fraud detection using an optimized light gradient boosting machine. IEEE Access, 8, 25579-25587.
Vairam, T., Sarathambekai, S., Bhavadharani, S., Dharshini, A.K., Sri, N.N., Sen, T. (2022), Evaluation of Naïve Bayes and Voting Classifier Algorithm for Credit Card Fraud Detection. In: Proceedings of the 8th International Conference on Advanced Computing and Communication Systems (ICACCS). p602-608.
Wickramanayake, B., Geeganage, D.K., Ouyang, C., Xu, Y. (2020), A Survey of Online Card Payment Fraud Detection Using Data Mining-based Methods. [arXiv preprint] arXiv:2011.14024.
Yang, R., Wang, P., Qi, J. (2023), A novel SSA-CatBoost machine learning model for credit rating. Journal of Intelligent and Fuzzy Systems, 44(2), 2269-2284.
Yanuar, R., Sa'adah, S., Yunanto, P.E. (2023), Implementation of hyperparameters to the ensemble learning method for lung cancer classification. Building of Informatics, Technology and Science (BITS), 5(2), 498-508.