Artificial Intelligence Applications And Innovations Vol. 1 No. 2 (2024)

Article history:
Received 10 January 2024
Revised 3 March 2024
Accepted 13 March 2024
Published online 02 April 2024

An optimal method using machine learning algorithms to detect fraud in banking services

Hodjat Hamidi[1]*, Milad Karbasiyan[1]

[1]Department of Industrial Engineering, Information Technology Group, K. N. Toosi University of Technology, Tehran, Iran

*** Corresponding author email address**: h_hamidi@kntu.ac.ir

A r t i c l e I n f o

Article type:
Original Research

How to cite this article:
Hamidi, H., & Karbasiyan, M., (2024). An optimal method using machine learning algorithms to detect fraud in banking services. Artificial Intelligence Applications and Innovations, *1*(2), 72-88.
https://doi.org/10.61838/jaiai.1.2.6

A B S T R A C T

In contemporary times, a substantial number of financial transactions and monetary transfers take place on the Internet and within electronic environments, thereby incentivizing fraudsters to infiltrate this domain. Consequently, the identification of individuals' identities in electronic service provision is exceedingly vital and crucial. This article aims to fraud detection in the banking system and present an optimal method utilizing artificial intelligence tools and model evaluation on the bank information of the Development and Cooperation Cooperative. In the initial phase, a gradient boosting algorithm, chosen for its high computational speed, is employed to train on a set of input data to identify and classify patterns of suspicious behaviors. In the second phase, an algorithm based on gradient boosting is utilized to refine results and optimize accuracy. To evaluate this approach, real data from a bank is employed, and the obtained results demonstrate that this method significantly enhances the speed and accuracy of fraud detection.

Keywords: *Fraud detection, banking transactions, machine learning algorithms, feature engineering, optimization, accuracy*

1. Introduction

Banks and financial institutions, due to the high costs associated with fraud, are striving to enhance speed and efficiency in identifying operations of fraudsters and deceivers. Fraud, as an illegal and unwarranted activity in the banking sector, poses a serious threat to the security and integrity of financial systems [1, 2]. Fraud in banking encompasses activities such as identity theft, financial fraud, the use of counterfeit credit cards, and the forgery of financial documents [3]. These activities lead to significant financial and reputational losses for both banks and their customers [4]. Examining the theoretical foundations of fraud in banking provides insight and a deeper understanding of this phenomenon and strategies to combat it. One method employed for detecting fraud in banking involves the use of machine learning. By employing this method, it is possible to categorize input transactions as valid or fraudulent based on the pattern of previous transactions. Sometimes, for detecting fraud in credit cards, simultaneous machine learning models and genetic algorithms are used. Additionally, the utilization of techniques such as convolutional neural networks and deep learning can be effective in fraud detection. Fraud in

banking is a serious issue that has led to the loss of millions of dollars in revenue for financial institutions worldwide [5]. Counteracting fraud in banking involves the use of machine learning and predictive analytics techniques. Algorithms such as artificial neural networks, decision trees, and genetic algorithms are employed for detecting fraud with credit cards [6]. Fraud in banking is executed through various methods. Common methods include phishing, card theft and/or loss, counterfeiting of fraudulent cards, and fraud with non-face-to-face cards. Phishing involves impersonating a legitimate entity and enticing customers into providing sensitive personal information, including usernames, passwords, and credit card details [7].

Given the high dependence on web technology in banking transactions, frauds related to banking have also increased. To combat the issue of fraud, there are various fraud detection methods and software applications that are utilized in industries such as credit cards, retail, e-commerce, insurance, and others. Among the effective methods for fraud detection in banking is data extraction technique, which examines the available information using mathematical algorithms to uncover possible evidence of fraud in the data [8]. Smart automation tools, leveraging advanced technologies and artificial intelligence algorithms, can analyze large volumes of data, identifying patterns and hidden maps in fraudulent behaviors. These tools can enhance fraud detection capabilities, reduce error rates, and improve security and trust in banking systems. This research, by presenting advanced and improved models for fraud detection, assists banks and financial organizations in more effectively combating fraud and establishing stronger security systems. Furthermore, this research holds economic significance as fraud and deception in banking result in significant financial losses for both banks and customers. On the one hand, public trust in financial and banking organizations is also affected. By utilizing advanced fraud detection models, it is possible to effectively prevent these losses and enhance customer trust. Therefore, this research, by examining and improving fraud detection models in banking and providing innovative solutions aligned with the needs of customers and financial organizations, contributes to improving security and trust in the banking sector. Additionally, it serves as a useful and practical guide for researchers and industry professionals interested in the fields of banking and information security, aiding in the development and progress of this domain.

In this article, a business intelligence-based model utilizing machine learning has been introduced, employing existing tools in business intelligence. The model aims to facilitate and expedite the fraud detection process by providing senior bank managers (who serve as the primary authorities in fraud management and detection within the bank) with information and analysis reports generated by fraud detection algorithms. In the second section, the research background is presented, followed by the research methodology in the third section, data analysis in the fourth section, and concluding with results, limitations, and research suggestions in the fifth section.

2. Background Research

Banking fraud refers to the violation of banking laws and regulations, encompassing behaviors such as misuse of information, credit fraud, loan fraud, and investment fraud [9].

Classification of frauds can be based on the type of fraudulent behavior, such as [10-14]:

- Credit Fraud: This type of fraud involves the misuse of banking credits for personal gain.
- Loan Fraud: This type of fraud includes obtaining loans using false information or misusing loans for illegal purposes.
- Banking Services Fraud: This type of fraud involves the misuse of banking services, creating fake banking services, and abusing banking service information.
- Electronic Transaction Fraud: This type of fraud includes the misuse of electronic transactions, engaging in illegal transactions, and exploiting transaction information.
- Gambling and Betting Fraud.

Methods for detecting banking fraud can include [10-16].

- Data Analysis: Using machine learning algorithms, banking data can be analyzed to identify fraudulent patterns.
- Alert Systems: These systems can identify suspicious activities and notify bank management.
- Internal Controls: This includes methods such as internal auditing and examining banking processes.

In [17], various methods, including classification, clustering, association rules, prediction, and sequence patterns, have been explored for fraud detection. In the classification method, algorithms based on decision trees and neural networks are employed. This method aids in the

classification of transactions and retrieves crucial information about the data. In the clustering method, similar banking transactions are grouped into clusters. This approach utilizes preprocessing and feature selection. The prediction method focuses on determining the relationship between dependent and independent variables, understanding changes in independent variables using regression analysis. This method is commonly used for fraud detection and prediction of threats in the banking system. Association rules aim to find sets of binary variables that frequently occur in the database. Neural networks are also used as a data extraction method, capable of extracting meaningful information from complex or common data and recognizing various patterns and sequences. Finally, the sequence patterns method is employed for data extraction, seeking similar patterns in given transactions over time and used for business analysis and detecting user purchasing behaviors.

In the article [18], an analysis and evaluation of various machine learning methods for fraud detection in credit card transactions have been conducted. The study utilizes algorithms such as Support Vector Machines, Polynomial Discriminant Analysis, Decision Trees, and Ensemble Learning algorithms.

Djakaria and Morris (2023), in their article titled "Artificial Intelligence Model as an Early Warning System for Fraudulent Transactions in Mobile Banking," investigate the impact of rapid technological development on the banking industry [19]. The focus of this article is the development of an artificial intelligence model designed for detecting fraudulent transactions within the domain of mobile banking. The data used to construct the artificial intelligence model encompasses mobile banking transactions from XYZ Bank in the year 2021. In [20], three convolutional neural network models have been developed for the detection of fraudulent bank accounts. All three models share a similar architecture, but they differ in the type of input features. Initially, commercial transaction records of the banking account history are fed into a directed transaction network, and weighted embedding is applied. Subsequently, a directed traversal algorithm is proposed for learning the account network vector.

In the article [21], an investigation is conducted into the application of advanced machine learning algorithms for fraud detection in credit card transactions. The authors employ data transformation methods, various classification algorithms, and modeling based on the previous records of credit card transactions. Their objective is to accurately detect all fraudulent transactions to prevent any oversight. Ultimately, the predictive results of different algorithms are examined, and a high-accuracy model is achieved. In essence, the use of machine learning algorithms facilitates the identification of fraudulent transactions. These algorithms automatically scrutinize a large number of payment requests and predict suspicious transactions. The examination results are further reviewed for assessing the model's accuracy, and adjustments to guidelines are implemented if necessary to prevent errors.

In [22], a combined analysis approach is employed to construct a robust predictive model. The experimental results indicate that the use of this combined approach improves accuracy and reduces errors in credit card fraud detection.

In [23], the article explores the latest methodologies and tools for fraud detection, analyzing a framework for implementing an advanced detection mechanism in the banking industry. By presenting an enhanced model for fraud detection, it assists banks and financial organizations in more effectively combating fraud and establishing stronger security systems.

In [24], the primary goal is the accurate classification of each transaction as legal or illegal. Therefore, to detect organized fraud in the network of banking transactions, an extensive data analysis has been employed. Additionally, a comparison between supervised learning algorithms has been presented on a dataset comprising 46,316 transactions related to customer card activities to distinguish between legal and illegal transactions. Based on metrics such as accuracy, prediction precision, recall (true positive detection rate), and F1 score, predictive models, including Random Forest and XGBoost, are considered suitable for fraud detection.

In [25], the authors delve into the analysis and examination of various methods used for identifying fraud in bank cards. Subsequently, a novel approach is presented that, leveraging advanced tools and techniques, can accurately detect fraud in bank cards. Finally, the results obtained from applying this new method to real-world data are presented, and its advantages and applications are thoroughly investigated. A summary of the relevant studies on various fraud detection methods and the results obtained is provided in Table 1.

Table 1

Summary of Research Conducted in Fraud Detection Methods

Author/Year	Method	Result
[1]	Comparison of fraud detection and anomaly detection techniques	Combining fraud detection and anomaly detection approaches improves fraud detection performance.
[10]	Combination of Neural Networks and Competitive Swarm Algorithm	98.54% accuracy in fraud detection.
[3]	Combination of NMF, Hierarchical k-means, K-means, KNN	Higher F-measure compared to Iforest, KNN, Median KNN, Average KNN.
[4]	Kohonen Network + Map Reduce	Reduction in execution time suitable for large-scale data.
[5]	Logistic Regression, KNN, Decision Tree, Random Forest, Gradient Boost	85% accuracy in credit card fraud detection.
[6]	Using Support Vector Machine and Enhanced Algorithms	Improved performance compared to other fraud detection methods.
[7]	Artificial Intelligence, Data Mining, and Location-Based Services	Introducing a model to reduce weaknesses in current fraud detection methods and increase accuracy.
[10]	Blockchain Technology and Logistic Regression, Support Vector Machine (SVM), Random Forest, XGBoost	Using blockchain technology is a better method for securing online transaction details. The Random Forest algorithm has a higher true positive rate compared to other models.
[11]	Various Machine Learning Algorithms	High-precision classification of fraudulent transactions.
[13]	Using Machine Learning Methods, "Decision Tree" and "K-Nearest Neighbors"	The KNN method performs better than DT and can be used to detect fraudulent activities in credit cards.
[19]	Utilizing Artificial Intelligence Model XGBoost	XGBoost model outperforms other models.
[22]	XGBoost Algorithm and LightGBM Algorithm	Significant improvement in speed and accuracy of fraud detection.
[23]	Various Machine Learning Algorithms	Random Forest and XGBoost algorithms are suitable predictive models for fraud detection.

3. Methodology

The primary objective of this research is to develop a precise and reliable model for predicting fraud in credit card transactions. In order to assess the efficiency and performance of the optimized model, steps have been taken to test and evaluate it on two distinct databases. The first database utilized is a sample from a European bank, encompassing financial information and customer transactions within a specific time frame. This database has been prepared with the aim of simulating real banking conditions.

For testing and evaluating the model on this database, the model's performance in detecting fraud has been compared with the available data in the sample database in the 'Class' field. The second database used in this research contains confidential information from “Banke To’se’ Taavon”. This database includes information on bank-to-bank card transactions over a one-month period and has limited access, requiring legal permissions and authorizations. Standard and reputable machine learning methods have been employed for testing and evaluating the optimized model.

To begin, the data has been divided into two sections, namely training and testing, to assess the model's performance under realistic conditions. Two primary sources have been utilized for data collection in this research. The first source is sample data from a European bank obtained from the Kaggle online platform. These data include information about European bank customers and have been used for training and evaluating machine learning models. The second set of data consists of real data from “Banke To’se’ Taavon”. To maintain data confidentiality, official authorization has been obtained from the relevant authority, ensuring the privacy of the data. These data, similar to the European bank data, have been used for testing and evaluating the final model.

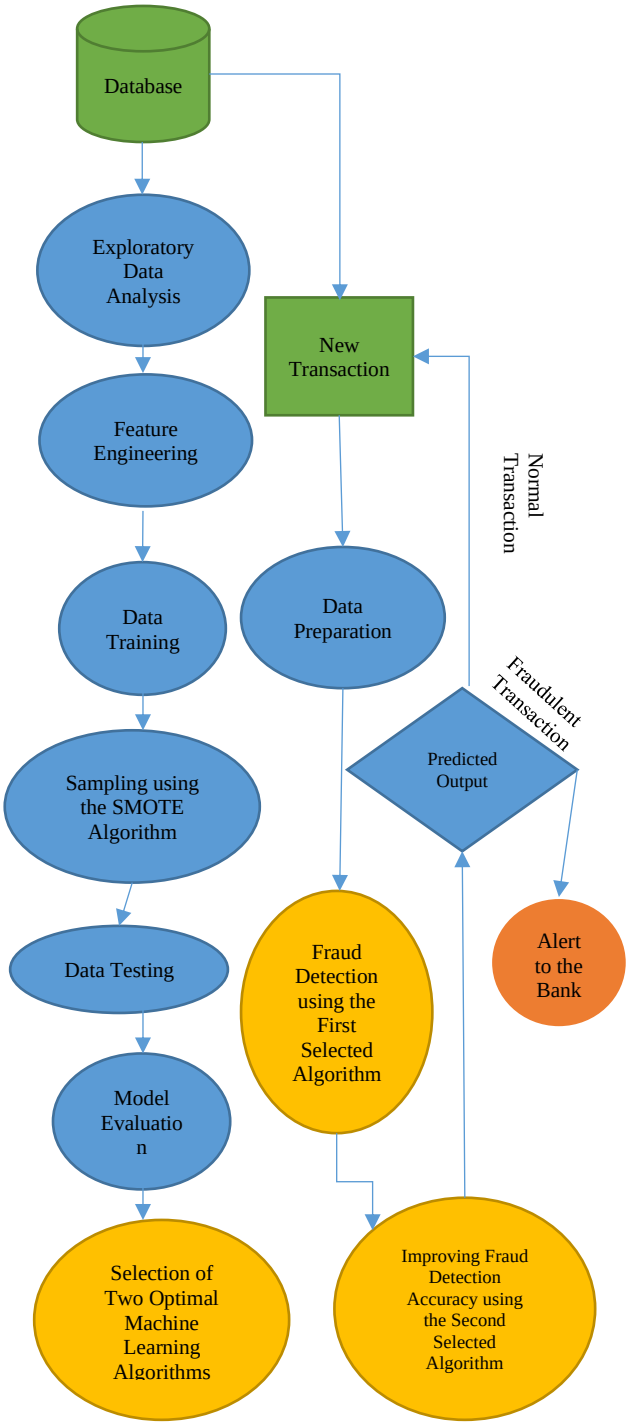

Figure 1

Proposal Framework

For feature selection, two sources have been consulted in this research. Initially, with the guidance of experts in the fields of banking and data analysis, important and influential features affecting the desired output have been identified. They, based on their experiences and technical knowledge, determined features related to bank customers. Then, suitable features were chosen using dependency analysis of these features. The European bank dataset consists of 284,807 records, of which 492 records are labeled as fraud. “Banke To’se’ Taavon” dataset comprises 4,153,053 records, with 5,161 records labeled as fraud. For data collection, preprocessing, and analysis, the Python

programming language and relevant libraries have been employed. Various machine learning algorithms, such as decision trees and random forests, have been used in the examination and evaluation of the data.

Proposal Framework Figure 1 is employed for fraud detection in card-to-card transactions (the model presented in [23]). The proposed framework, utilizing the XGBoost and LightGBM algorithms, incorporates a sequential approach to enhance accuracy. In the proposed sequential model, initially, the XGBoost algorithm is applied to the data from "Banke To'se' Taavon" to efficiently and accurately identify outlier samples.

Subsequently, the LightGBM algorithm is applied to the output filtered by the XGBoost algorithm to eliminate some cases that may be incorrectly identified as fraud (false positives, FP). Considering the conducted evaluations, both algorithms exhibit high accuracy. Since XGBoost outperforms LightGBM significantly in terms of speed, the first priority is given to the execution of the XGBoost algorithm. To address the speed deficiency of the LightGBM algorithm, it is employed in the second stage with a substantially reduced dataset.

By sequentially utilizing the XGBoost and LightGBM algorithms, the capability to identify outlier samples with high accuracy in "Banke To'se' Taavon" dataset is established. This sequence has resulted in a precise model with high execution speed for predicting information from "Banke To'se' Taavon."

The first research population includes credit card transactions of a European bank, as per the sample data in Figure 2, spanning two days in the year 2013. The second research population comprises card-to-card transactions conducted in "Banke To'se' Taavon" over one month.

4. Data Analysis

To prepare the data and initiate learning and testing, activities such as exploratory data analysis, loading and quality adjustment of the data, feature selection, and data transformation must be performed. Figure 2

Sample dataset related to a European bank

illustrates the preprocessed data for the European bank information. To scale the data, the SMOTE algorithm has been employed. This algorithm is used for synthetic data generation for rare classes to maintain balance between classes and reduce differences in the number of samples among classes. The use of The SMOTE can significantly enhance the performance of machine learning algorithms.

	Time	V1	V2	V3	...	V27	V28	Amount	Class
0	0.0	-1.359807	-0.072781	2.536347	...	0.133558	-0.021053	149.62	0
1	0.0	1.191857	0.266151	0.166480	...	-0.008983	0.014724	2.69	0
2	1.0	-1.358354	-1.340163	1.773209	...	-0.055353	-0.059752	378.66	0
3	1.0	-0.966272	-0.185226	1.792993	...	0.062723	0.061458	123.50	0
4	2.0	-1.158233	0.877737	1.548718	...	0.219422	0.215153	69.99	0

[5 rows x 31 columns]

Figure 2

Sample dataset related to a European bank

```
            Time        V1        V2  ...       V28  Amount  Class
33          26.0 -0.529912  0.873892  ...  0.023307    6.14      0
35          26.0 -0.535388  0.865268  ...  0.025427    1.77      0
113         74.0  1.038370  0.127486  ...  0.001192    1.18      0
114         74.0  1.038370  0.127486  ...  0.001192    1.18      0
115         74.0  1.038370  0.127486  ...  0.001192    1.18      0
...          ...       ...       ...  ...       ...     ...    ...
282987  171288.0  1.912550 -0.455240  ... -0.036020   11.99      0
283483  171627.0 -1.464380  1.368119  ...  0.119251    6.82      0
283485  171627.0 -1.457978  1.378203  ...  0.116772   11.93      0
284191  172233.0 -2.667936  3.160505  ... -0.222200   55.66      0
284193  172233.0 -2.691642  3.123168  ... -0.213020   36.74      0

[1081 rows x 31 columns]
            Time         V1         V2  ...       V28  Amount  Class
0            0.0  -1.359807  -0.072781  ... -0.021053  149.62      0
1            0.0   1.191857   0.266151  ...  0.014724    2.69      0
2            1.0  -1.358354  -1.340163  ... -0.059752  378.66      0
3            1.0  -0.966272  -0.185226  ...  0.061458  123.50      0
4            2.0  -1.158233   0.877737  ...  0.215153   69.99      0
...          ...        ...        ...  ...       ...     ...    ...
284802  172786.0 -11.881118  10.071785  ...  0.823731    0.77      0
284803  172787.0  -0.732789  -0.055080  ... -0.053527   24.79      0
284804  172788.0   1.919565  -0.301254  ... -0.026561   67.88      0
284805  172788.0  -0.240440   0.530483  ...  0.104533   10.00      0
284806  172792.0  -0.533413  -0.189733  ...  0.013649  217.00      0

[283726 rows x 31 columns]
Class
0    284315
1       492
```

Figure 3

Pre-processed sample data related to a European bank

At this stage, crucial and impactful data have been selected considering features and expert opinions (Figure 4). For “Banke To’se’ Taavon”, the number of daily and monthly card transactions as the source and destination has also been considered (the distribution of some feature data concerning the amount is illustrated in Figure 5).

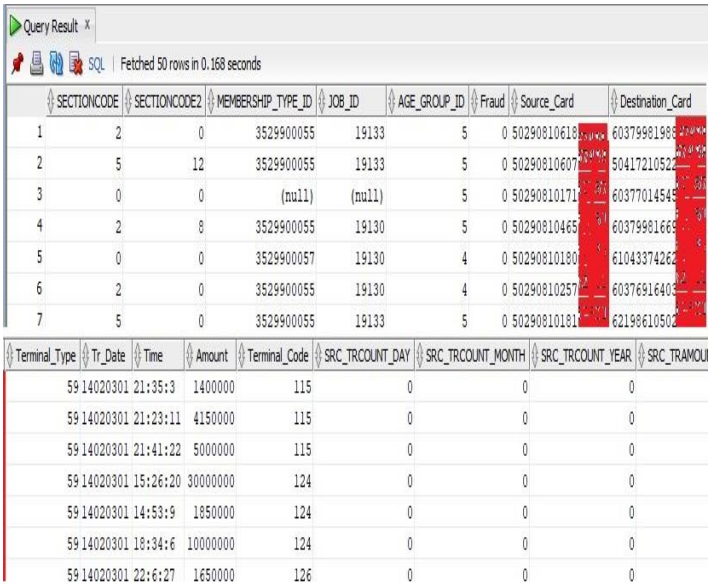

Figure 4

Feature selection from the actual dataset of “Banke To’se’ Taavon”

Figure 5

The distribution of data for some features relative to the amount

The distribution ratio of the number of transactions across different amounts is depicted in Figure 6, representing the frequency of certain amounts in specific ranges. Additionally, the transaction volume at different hours of the day is illustrated in Figure 7.

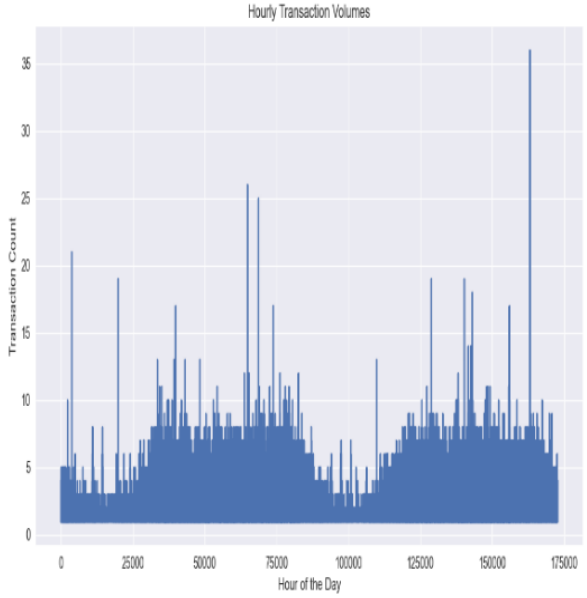

Figure 6

The distribution ratio of the number of transactions across different amounts

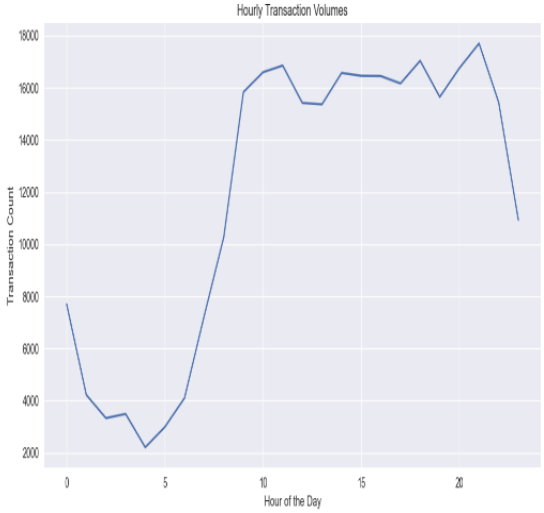

Figure 7

The distribution ratio of the number of transactions across different amounts

After calculating the correlation coefficient for the relationship between amount-related features and the class (fraud label), as well as with other features, the coefficients, ranging between -1 and 1, are indicated in Figure 8.

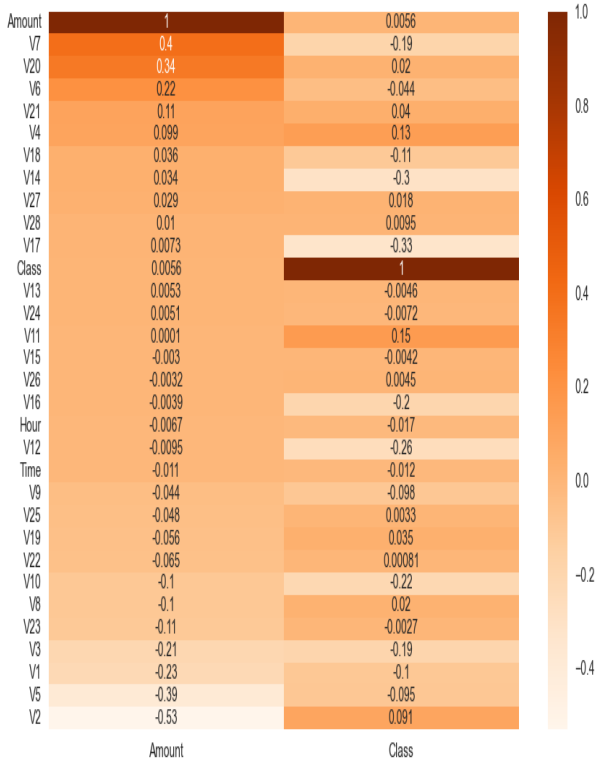

Figure 8

The correlation between amount-related features and fraud labels with other features of a European bank

Evaluation of the Proposed Algorithm's Performance in Distinguishing Normal and Abnormal Behaviors requires defining some numerical metrics to express the quality of correct labeling. For this purpose, let's assume there are P records with a positive label and N records with a negative label in a given dataset. Algorithm X aims to re-label the records in this dataset. If the label assigned by algorithm X to each record is the same as its true label, algorithm X has made a correct detection; otherwise, it has made an incorrect detection.

The goal here is to evaluate the labeling power of algorithm X. Based on this, before defining evaluation metrics, four basic concepts named True Positive (TP), True Negative (TN), False Positive (FP), and False Negative (FN) need to be defined. TP represents the number of records that algorithm X correctly assigned a positive label. TN indicates the number of records that algorithm X correctly assigned a negative label. FP denotes the number of records whose actual label is negative, but algorithm X mistakenly assigned a positive label. Finally, FN represents the number of records whose actual label is positive, but algorithm X mistakenly assigned a negative label (Table 2).

Table 2

Displaying the four fundamental concepts in assessing the discriminative power of an algorithm [26].

Real Label / X Label	Positive	Negative
Positive	True Positive (TP)	False Positive (FP)
Negative	False Negative (FN)	True Negative (TN)
AND (Binary)	Positive	Negative

To evaluate the performance of the algorithms, the dataset has been randomly divided into two sets: a training set and a test set. The training dataset is utilized for training the algorithms, while the test dataset is employed to assess their performance.

4.1. Evaluation Metrics

- F1 Score: A metric combining precision and recall, commonly used for comparing algorithms.
- Receiver Operating Characteristic (ROC) Curve: A graph showing the relationship between the true positive rate and false positive rate (ROC-AUC).
- Confusion Matrix: A table indicating the number of instances correctly and incorrectly classified by the algorithm.

4.2. XGBoost Algorithm without the SMOTE

The XGBoost algorithm without using the SMOTE technique has demonstrated very satisfactory performance in the analysis and prediction of data (Figure 9). For the test set, the ROC-AUC value is 0.8928, indicating the model's high accuracy and efficiency. Additionally, accuracy (Acc), precision (TP), recall, and F1 score are all very high and equal to 0.9996. These results indicate that the algorithm is capable of accurately predicting positive and negative labels in the data.

The AUC value is 0.8928, showing the algorithm's ability to distinguish between classes. This value is close to 1, indicating the algorithm's discriminative power. In the confusion matrix, the number of true positives (TP) is 77, the number of true negatives (TN) is 86256, the number of false positives (FP) is 2, and the number of false negatives (FN) is 21. These results demonstrate that the algorithm has the ability to correctly detect between classes, and the number of incorrect errors has been minimized.

The processing time for this analysis with the XGBoost algorithm is approximately 28.6 seconds, indicating that the XGBoost algorithm is generally fast and efficient.

By optimizing the parameters, the best hyperparameter values for this XGBoost algorithm have been determined according to Equation (1).

Equation 1. XGBoost algorithm best hyperparameter

- 'learning_rate': 0.8
- 'max_depth': 5
- 'subsample': 0.9

These parameters have significantly improved the performance of the XGBoost algorithm, leading to an increase in accuracy and model efficiency.

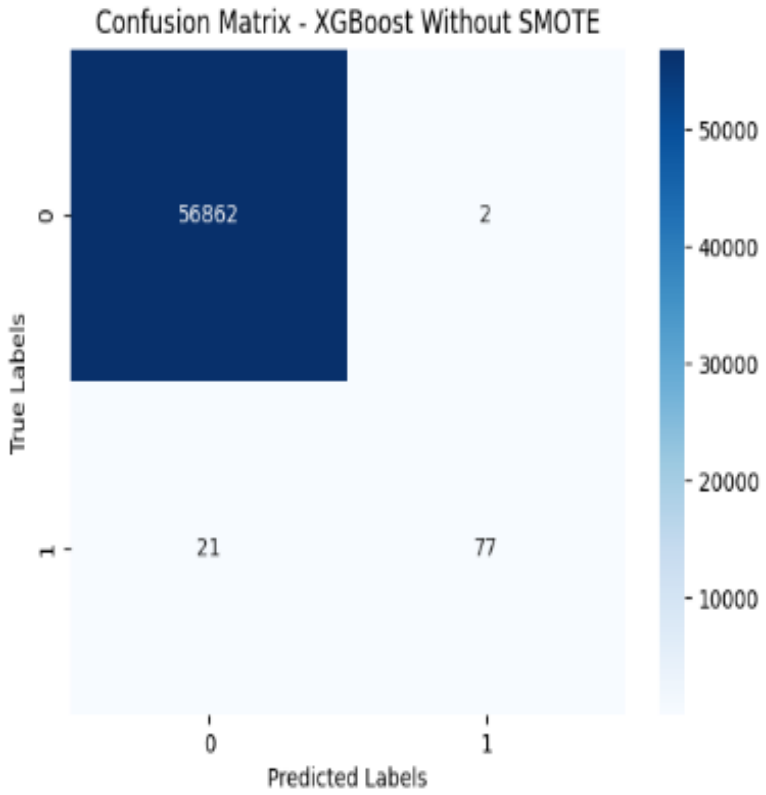

Figure 9

Confusion matrix of the XGBoost algorithm without SMOTE

4.3. XGBoost Algorithm with the SMOTE

The XGBoost algorithm, utilizing the SMOTE technique, has also yielded highly favorable results in data analysis and prediction (Figure 10). For the test set, the ROC-AUC value is 0.928, indicating the model's high accuracy and efficiency in distinguishing between classes. Additionally, accuracy (Acc), positive predictive accuracy, recall, and F1 score are all very high, at 0.9996. These results demonstrate that the algorithm, when using The SMOTE, is capable of better detection and prediction of positive and negative labels in the data. The AUC value of 0.928 further signifies the algorithm's ability to discriminate and differentiate between classes, with a value close to 1 indicating excellent performance. In the confusion matrix, the number of correctly selected positive samples (TP) is 84, and the number of correctly rejected samples (TN) is 853.56. Furthermore, the number of incorrectly selected samples (FP) is 11, and the number of incorrectly rejected samples (FN) is 14. These results indicate that the algorithm, when using The SMOTE, has a better ability to correctly distinguish between classes and reduce false errors. The processing time of the algorithm using The SMOTE is approximately 91.16 seconds, indicating that the use of this technique requires more time but comes with an improved algorithm performance. Through parameter optimization, the best hyperparameter values for this XGBoost algorithm have been determined according to Equation (1). These parameters have led to a significant improvement in the performance of the XGBoost algorithm, resulting in increased accuracy and model efficiency.

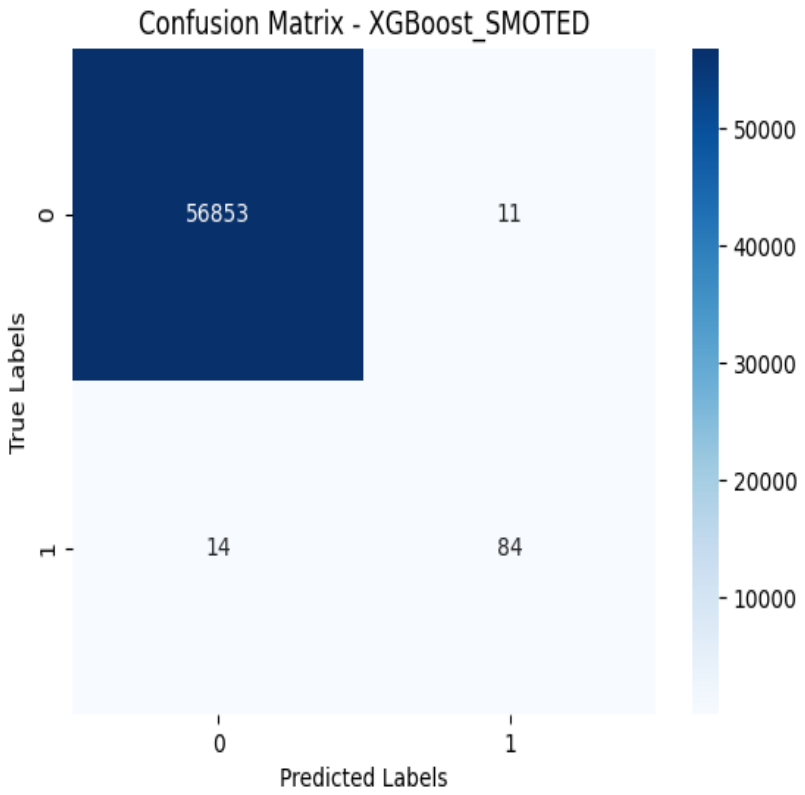

Figure 10

Confusion matrix of the XGBoost algorithm with SMOTE

4.4. The Decision Tree algorithm without the SMOTE

The Decision Tree algorithm, without using the SMOTE technique, has provided acceptable results in data analysis and prediction (Figure 11). For the test set, the ROC-AUC value is 0.8928, indicating the model's accuracy and efficiency in distinguishing between classes. Additionally, accuracy (Acc), positive predictive accuracy, recall, and F1 score are all relatively high, at 0.9994. These results demonstrate that the algorithm has a high capability to detect and predict positive and negative labels in the data. The AUC value of 0.8928 further signifies the algorithm's ability to discriminate and differentiate between classes, with a value close to 1 indicating acceptable performance. In the confusion matrix, the number of correctly selected positive samples (TP) is 77, and the number of correctly rejected samples (TN) is 56852. Furthermore, the number of incorrectly selected samples (FP) is 12, and the number of incorrectly rejected samples (FN) is 21. These results indicate that the algorithm has the ability to correctly distinguish between classes, and the number of false errors has been minimized. The processing time of the Decision Tree algorithm for this analysis is approximately 8.7605 seconds, indicating that the Decision Tree algorithm has fast performance.

By optimizing the parameters, the best hyperparameter values for this Decision Tree algorithm have been determined according to Equation:(۲)

Equation 2. Decision Tree algorithm best hyperparameter

- 'criterion': 'entropy'
- 'max_depth': 3
- 'min_samples_leaf': 1
- 'min_samples_split': 2

These parameters have significantly improved the performance of the Decision Tree algorithm, leading to an increase in accuracy and model efficiency.

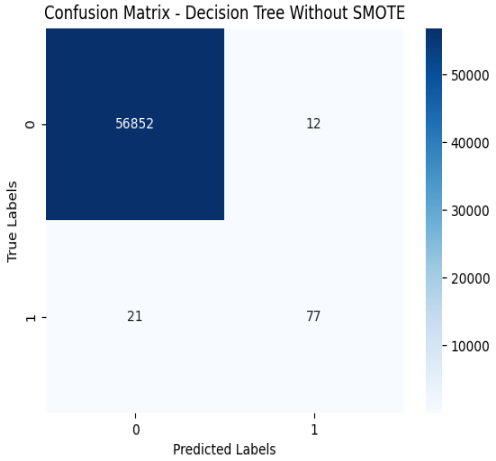

Figure 11

Confusion matrix of the decision tree algorithm without SMOTE

4.5. The Decision Tree algorithm with the SMOTE

The decision tree algorithm, when coupled with the SMOTE, has demonstrated significantly superior outcomes in the analysis and prediction of data (Figure 12). The model accuracy reached 0.9981, with positive prediction accuracy, recall, and F1 score also standing at 0.9981, respectively. The confusion matrix further indicates that the number of correctly selected instances is 56.782, while the number of correctly rejected instances is 75. Conversely, the number of incorrectly selected instances is 82, with 23 instances incorrectly rejected. These findings affirm that the decision-making algorithm, when employing The SMOTE, successfully discriminates between classes and mitigates misclassification errors. The processing time for the algorithm using The SMOTE was approximately 110.83 seconds, underscoring the increased time requirement associated with this technique. However, this additional time investment is justified by the improved algorithmic performance. Through parameter optimization, the optimal hyperparameter values for this algorithm are determined in accordance with Equation (2).

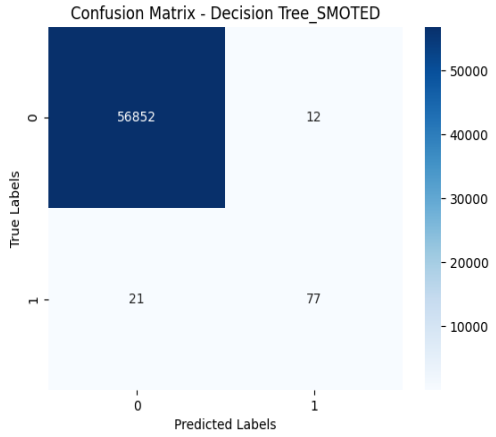

Figure 12

Confusion matrix of the decision tree algorithm with SMOTE

4.6. *Isolation-based Random Forest Algorithm without SMOTE*

The Isolation-based Random Forest algorithm, devoid of the application of the SMOTE, has yielded satisfactory results in the analysis and prediction of data (Figure 13). The ROC-AUC value on the test set is 0.9092, indicating the algorithm's capability in discrimination and differentiation between classes. The model accuracy is 0.9510, with positive prediction accuracy, recall, and F1 score also standing at 0.9510, respectively. The AUC value is also 0.9092, demonstrating the algorithm's effectiveness in distinguishing and segregating between classes. The confusion matrix further reveals that the number of correctly selected instances is 54,086, while the number of correctly rejected instances is 85. Conversely, the number of incorrectly selected instances is 2,778, with 13 instances incorrectly rejected. These findings underscore the Isolation-based Random Forest algorithm's adeptness in class discrimination and reduction of misclassification errors without the utilization of SMOTE. The processing time for the algorithm without SMOTE is approximately 4.8042 seconds, indicating that the algorithm runs within an acceptable time frame.

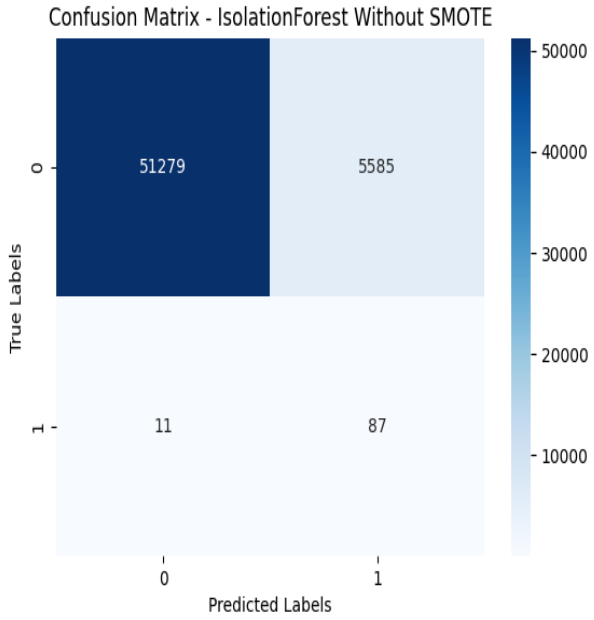

Figure 13

Confusion matrix of the Isolation Random Forest algorithm without SMOTE

4.7. *Isolation-based Random Forest Algorithm Utilizing SMOTE Technique*

The Isolation-based Random Forest algorithm, integrated with the SMOTE, has yielded moderate results in the analysis and prediction of data (Figure 14). The ROC-AUC value on the test set is 0.6295, indicating the algorithm's capability in discrimination and differentiation between classes. The model accuracy is 0.9924, with positive prediction accuracy, recall, and F1 score also standing at 0.9924, respectively. The AUC value is also 0.6295, demonstrating the algorithm's effectiveness in distinguishing and segregating between classes. The confusion matrix further reveals that the number of correctly selected instances is 56,504, while the number of correctly rejected instances is 26. Conversely, the number of incorrectly selected instances is 360, with 72 instances incorrectly rejected. These findings highlight that the Isolation-based Random Forest algorithm, when utilizing SMOTE, possesses a moderate capability in class discrimination and reduction of misclassification errors. The processing time for the algorithm with SMOTE is

approximately 8.4067 seconds, indicating that the algorithm runs within an acceptable time frame.

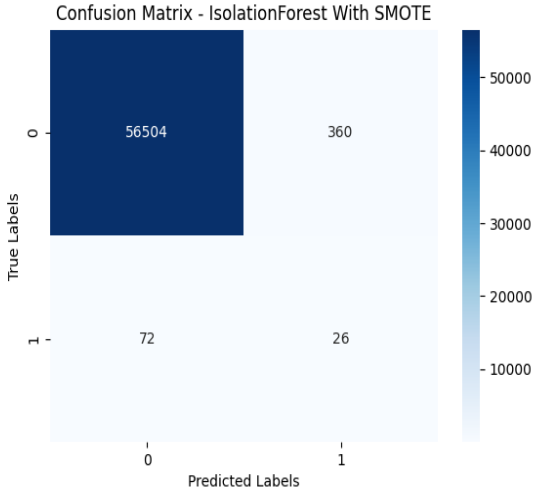

Figure 14

Confusion matrix of the Isolation Random Forest algorithm with SMOTE

4.8. LightGBM Algorithm without SMOTE

The LightGBM algorithm, implemented without the application of the SMOTE, has yielded highly favorable results in the analysis and prediction of data (Figure 15). The ROC-AUC value on the test set is 0.9030, indicating the algorithm's high proficiency in discrimination and differentiation between classes. The model accuracy is 0.9996, with positive prediction accuracy, recall, and F1 score also standing at 0.9997, 0.9518, 0.8061, and 0.8729, respectively. The AUC value is also 0.9030, demonstrating the algorithm's effectiveness in distinguishing and segregating between classes. The confusion matrix further reveals that the number of correctly selected instances is 56,860, while the number of correctly rejected instances is 79. Conversely, the number of incorrectly selected instances is 4, with 19 instances incorrectly rejected. These results underscore that the LightGBM algorithm, when implemented without SMOTE, exhibits a highly proficient capability in class discrimination and reduction of misclassification errors. The processing time for the algorithm without SMOTE is approximately 131.6849 seconds, indicating that the algorithm runs within an acceptable time frame.

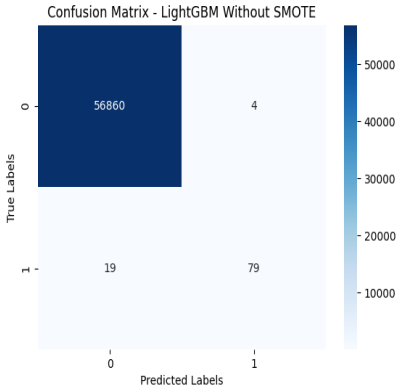

Figure 15

Confusion Matrix - LightGBM without SMOTE

5. Conclusion

Despite the various tools employed by banks for fraud prevention, novel methods for detecting fraud in banking continue to require development. In this article, a new model for fraud detection in banking utilizing artificial intelligence tools has been presented. Subsequently, using machine learning algorithms, a new model for fraud detection in banking has been developed. In this model, banking data is utilized, and through machine learning algorithms, it is determined whether a transaction is identified as fraudulent or not. In the end, the performance of the proposed model is examined using real-world data, demonstrating that the presented model can accurately identify fraudulent transactions.

The presented method consists of two main stages. In the first stage, transaction information is preprocessed and entered into the XGBoost and SMOTE hybrid algorithm to identify frauds. In the second stage, the filtered information is entered SMOTE hybrid algorithm to enhance the accuracy of fraud detection. This stage leads to a significant improvement in fraud detection accuracy. The results indicate that sequential machine learning models contribute to enhancing performance in fraud detection in the banking system. The proposed model is capable of accurately and reliably detecting fraud in a cooperative bank, with an accuracy rate of 99.87% for negatives and 64% for positives. Given the flexibility in model design, the proposed model has the potential for transferability and use in other financial organizations.

Given the following suggestions, future research endeavors can contribute to the enhancement and expansion of fraud detection methods in financial transactions, thereby aiding in the improvement of security and efficiency of financial systems:

Utilization of Advanced Algorithms and Models: To enhance the accuracy and performance of models, employing newer and more sophisticated algorithms and models is recommended. This encompasses the use of deep neural networks and reinforcement learning methods.

- Development of Multi-Class Models: In this study, a model has been designed to identify two fraud states and non-fraud instances. Future research can extend multi-class models to detect various types of fraudulent transactions, such as credit card fraud, identity theft, and others.
- Integration of Multiple Models: Combining several different models for fraud detection can be beneficial. This approach may contribute to improving the accuracy and reliability of the model compared to the use of a single model.
- Real-time Implementation of Fraud Detection Methods: While the current study trained the model on historical data, future research could implement fraud detection methods in real-time, providing instantaneous identification upon the occurrence of a transaction.
- Conducting Further Research in Related Areas: In-depth exploration and research in related domains such as cybersecurity, encryption, big data analytics, and artificial intelligence can advance and enhance fraud detection methodologies.

Authors' Contributions

Declaration

None.

Transparency Statement

Acknowledgments

Declaration of Interest

Funding

Ethical Considerations

References

[1] H. Hamidi and R. Moradi, "Design of a dynamic and robust recommender system based on item context, trust, rating matrix and rating time using social networks analysis," *Journal of King Saud University-Computer and Information Sciences*, vol. 36, no. 2, p. 101964, 2024, doi: 10.1016/j.jksuci.2024.101964.

[2] A. Cherif, A. Badhib, H. Ammar, S. Alshehri, M. Kalkatawi, and A. Imine, "Credit card fraud detection in the era of disruptive technologies: A systematic review," *Journal of King Saud University-Computer and Information Sciences*, vol. 35, no. 1, pp. 145-174, 2023, doi: 10.1016/j.jksuci.2022.11.008.

[3] A. Cherif, H. Ammar, M. Kalkatawi, S. Alshehri, and A. Imine, "Encoder–decoder graph neural network for credit card fraud detection," *Journal of King Saud University-Computer and Information Sciences*, vol. 36, no. 3, 2024, doi: 10.1016/j.jksuci.2024.102003.

[4] H. Hamidi and A. Chavoshi, "Social, Individual, Technological and Pedagogical Factors Influencing Mobile Learning Acceptance in Higher Education: A Case from Iran," *Telematics and Informatics*, 2019, doi: 10.1016/j.tele.2018.09.007.

[5] D. Sharma and S. Singh Kang, "Hybrid model for detection of frauds in credit cards," 2022, pp. 70-77, doi: 10.1109/ICAC3N56670.2022.10074057.
[6] S. K. Hashemi, S. L. Mirtaheri, and S. Greco, "Fraud Detection in Banking Data by Machine Learning Techniques," *IEEE Access*, vol. 11, pp. 3034-3043, 2023.
[7] K. Nkomo and T. Breetzke, "A conceptual model for the use of artificial intelligence for credit card fraud detection in banks," 2020, doi: 10.1109/ICTAS47918.2020.233980.
[8] S. Patil, V. Nemade, and P. Soni, "Predictive Modelling For Credit Card Fraud Detection Using Data Analytics," 2018, vol. 132, pp. 385-395, doi: 10.1016/j.procs.2018.05.199.
[9] H. Hamidi and M. Safareyeh, "A model to analyze the effect of mobile banking adoption on customer interaction and satisfaction: a case study of m-banking in Iran," *Telematics and Informatics*, 2019, doi: 10.1016/j.tele.2018.09.008.
[10] E. M. S. W. Balagolla, W. P. C. Fernando, and R. M. N. S. Rathnayake, "Credit Card Fraud Prevention Using Blockchain," 2021, doi: 10.1109/I2CT51068.2021.9418192.
[11] J. S. Kirar, D. Kumar, and D. Chatterjee, "Exploratory Data Analysis for Credit Card Fraud Detection," 2021, pp. 157-161, doi: 10.1109/ComPE53109.2021.9751922.
[12] L. Bahrami, N. Safaie, and H. Hamidi, "Effect of motivation, opportunity and ability on human resources information security management considering the roles of Attitudinal, behavioral and organizational factors," *International Journal of Engineering, Transactions C: Aspects*, vol. 34, no. 12, pp. 2624-2635, 2021, doi: 10.5829/ije.2021.34.12c.07.
[13] R. O. Ogundokun, S. Misra, O. E. Ogundokun, J. Oluranti, and R. Maskeliunas, "Machine Learning Classification Based Techniques for Fraud Discovery in Credit Card Datasets," 2021, pp. 26-38, doi: 10.1007/978-3-030-89654-6_3.
[14] S. Daliri, "Using Harmony Search Algorithm in Neural Networks to Improve Fraud Detection in Banking System," *Computational Intelligence and Neuroscience*, vol. 2020, p. 6503459, 2020, doi: 10.1155/2020/6503459.
[15] F. S. Esmail, F. K. Alsheref, and A. E. Aboutabl, "International journal of electrical and computer engineering systems," *International Journal of Electrical and Computer Engineering Systems*, vol. 14, no. 2, pp. 229-239, 2023, doi: 10.32985/ijeces.14.2.12.
[16] D. R. Rambola, P. Varshney, and P. Vishwakarma, "Data Mining Techniques for Fraud Detection," 2018, doi: 10.1109/CCAA.2018.8777535.
[17] B. K. Padhi, S. Chakravarty, and B. N. Biswal, "Anonymized Credit Card Transaction Using Machine Learning Techniques," in *Advances in Intelligent Computing and Communication*, vol. 109: Springer Nature Singapore Pte Ltd., 2020, pp. 413-423.
[18] H. Hamidi and A. Tavassoli, "A Model for Scheduling of Electric Vehicles Charging in a Distribution Network using Multi-Agent Model," *International Journal of Engineering, Transactions B: Applications*, vol. 37, no. 2, pp. 402-411, 2024.
[19] M. Djakarta and T. Mauritsius, "Artificial Intelligence Model as an Early Warning System for Fraudulent Transactions in Mobile Banking," *ICIC International, Part B: Applications*, vol. 14, no. 7, pp. 747-753, 2023, doi: 10.24507/icicelb.14.07.747.
[20] V. V. H. Pham *et al.*, "PaaS-black or white: An investigation into software development model for building retail industry SaaS," 2017, pp. 285-287, doi: 10.1109/ICSE-C.2017.57.
[21] I. Vorobyev and A. Krivitskaya, "Reducing false positives in bank anti-fraud systems based on rule induction in distributed tree-based models," *Computers & Security*, vol. 120, 2022.
[22] H. Hamidi and M. Karbasian, "Presenting a model to detect the fraud in banking using smart enabling tools: Case Study One of the State banks of Iran," *International Journal of Engineering*, vol. 37, no. 3, pp. 529-537, 2024.
[23] S. Khosravi and M. Kargari, "Using Supervised Machine Learning Approaches To Detect Fraud In The Banking Transaction Network," 2023, pp. 115-119, doi: 10.1109/ICWR57742.2023.10139083.
[24] H. Hamidi and S. H. Seyed Lotfali, "Analysis of Role of Cloud Computing in Providing Internet Banking Services: Case Study Bank Melli Iran," *International Journal of Engineering*, vol. 35, no. 5, pp. 1082-1088, 2022, doi: 10.5829/ije.2022.35.05b.23.
[25] A. Torabi, H. Hamidi, and N. Safaie, "Effect of Sensory Experience on Customer Word-of-Mouth Intention, Considering the Roles of Customer Emotions, Satisfaction, and Loyalty," *International Journal of Engineering*, vol. 34, no. 3, pp. 682-699, 2021, doi: 10.5829/ije.2021.34.03c.13.
[26] A. Alvanchi, N. Didehvar, M. Jalilehvand, P. Adami, and S. Shahmi, "Semi-Augmented Reality, a Novel Approach to Improve Customer Safety in the Pre-sale Process of Under Construction Buildings," *International Journal of Engineering*, vol. 34, no. 10, pp. 2198-2205, 2021.