IJE TRANSACTIONS C: Aspects Vol. 37 No. 03, (March 2024) 529-537

International Journal of Engineering

Journal Homepage: www.ije.ir

Presenting a Model to Detect the Fraud in Banking using Smart Enabling Tools

M. Karbasiyan[1,2], H. Hamidi*[1,2]

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

P A P E R I N F O

Paper history:
Received 13 November 2023
Received in revised form 22 November 2023
Accepted 26 November 2023

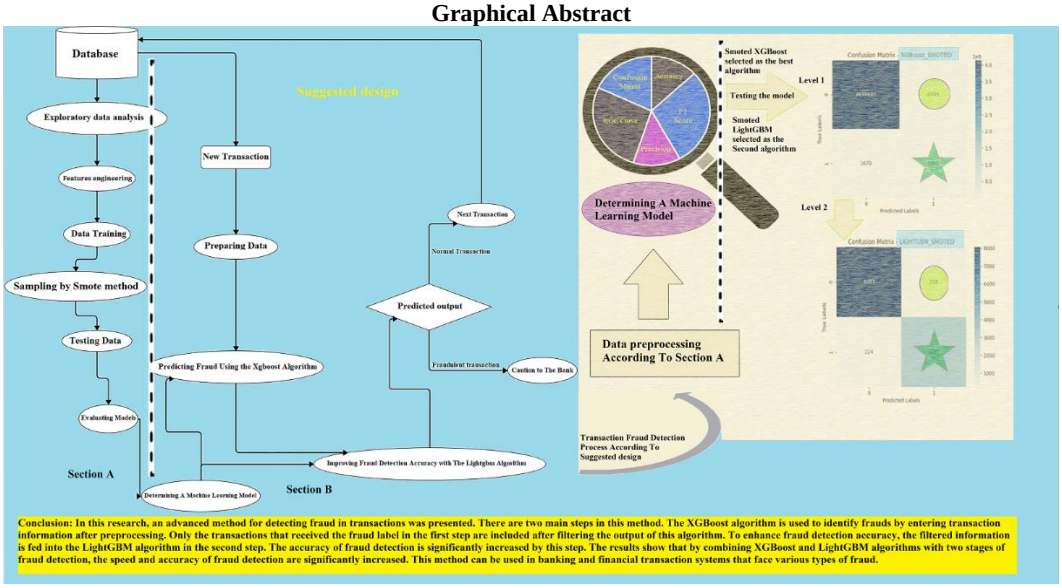
Keywords:
Bank Fraud Detection
Intelligent Model
Tose'e ta'avon Bank
XGBoost Algorithm
LightGBM Algorithm
F and ROC Criteria

A B S T R A C T

In recent years, with the increase of access to customer data and the improvement of data analysis capabilities through intelligent methods, various activities have been carried out to analyze customer behavior; it is in the detection of bank frauds. Currently, bank frauds have a wide range of results, other than material and financial losses to the bank, customers and banks. After using smart tools to use different algorithms, the two selected algorithms XGBoost and LightGBM, according to the high ROC in the obtained models were selected step by step. At the same time, it has been used in final tests with the reduction of false samples labeled as fraud (FP). This model is developed using real development data and gives very acceptable results in card-to-card fraud detection. This model can significantly improve the security of the banking system and be used as a tool to reduce financial crimes.

***doi**: 10.5829/ije.2024.37.03c.10*

Graphical Abstract



1. INTRODUCTION

Fraud, which is a multi-million-dollar business worldwide, has become a significant problem nowadays. The development of new technologies has resulted in the creation of new ways to commit fraud. The creation of a new information system, in addition to its advantages and benefits, can create additional opportunities for

*Corresponding Author Email: h_hamidi@kntu.ac.ir (H. Hamidi)

Please cite this article as: Karbasiyan M, Hamidi H, Srinivasa Rao K. Presenting a Model to Detect the Fraud in Banking using Smart Enabling Tools. International Journal of Engineering, Transactions C: Aspects. 2024;37(03):529-37.

criminals. In addition to detecting fraud and fraud in organizations, fraud detection techniques and intelligence tools aim to predict future behavior and reduce the risk of fraud by understanding user and customer behavior. Banks and financial institutions are striving to speed up the process of identifying fraudsters due to the high costs of fraud (1-3). It is against the law to commit fraud in electronic banking and electronic money transfer. Fraudsters are encouraged and incited to enter this field due to the large volume of monetary and financial transactions and transfers conducted on the Internet and electronic platform (4-6). To provide electronic services, it is crucial and important to recognize the identity of individuals. The purpose of this study was to uncover fraud in the banking system and develop an optimal method for analyzing information from the One of the State banks of Iran using intelligence tools and model evaluation. The focus of this research is to review the latest fraud detection methodologies and tools. The propose of this is to develop the framework for the fraud detection mechanism, as well as the use of the Python language to implement the developed model. In the following, according to the research literature and the background of the research, there is an introduction about the previous studies and different methods of fraud detection, in the next part, the proposed research plan and research methodology, and then the analysis of the information and the research results are given.

2. LITERATURE REVIEW

An introduction to fraud and fraud detection methods is provided in this preliminary section, based on previous studies. The increase in communication technologies and online transactions has led to an increase in financial frauds. One of the most common and dangerous forms of financial fraud is credit card fraud. Machine learning algorithms and neural networks can be used to detect patterns and anomalies related to fraud in mobile banking transactions (7-10). Artificial intelligence-based systems are able to detect and prevent fraud in real time due to the increasing number of financial frauds in the banking industry and the significant financial losses caused to banks and their customers, which is a significant advantage over traditional fraud detection methods. Real-time performance is what all AI-based systems have in common. Using machine learning algorithms and neural networks, these systems are capable of identifying fraudulent patterns and behaviors in mobile banking transactions and taking preventive measures if fraud is detected. Fraud detection systems can model customer behavior patterns based on past transaction history and other factors like location, time, and type of transactions. Then, if anomalous behavior or suspicious transactions are detected, the system activates an alert. To review and verify the transactions, the bank or customer can receive this alert as a text message or notification (11-15).

The detection and identification of fraudulent activities in credit card transactions can be achieved through the use of machine learning and data mining methods. The importance of this issue is because the use of credit cards in payments is increasing worldwide. Fraud detection is done in all three classical, online, and commercial fields through data mining and machine learning (16-19). Banking and other related industries face a significant challenge in detecting and preventing fraud. Companies use data analysis and machine learning algorithms to identify patterns and suspicious behaviors. There is no complete and effective solution for fraud detection in banking and e-commerce yet, and there are problems like false positive results and reduced system accuracy (20-23). Advanced fraud detection models can be very effective in dealing with fraud in e-commerce. As an intelligent system, these models are capable of identifying fraud patterns and recognizing suspicious transactions. Using advanced methods like machine learning and artificial intelligence can improve fraud detection and prevent financial and credit losses caused by fraud in e-commerce (24-26). The financial industry has been able to use better and more effective fraud detection methods; thanks to the development and advancement of various technologies and their combination with big data analysis and artificial intelligence. The detection and prevention of fraud in the financial industry can be significantly improved by integrating these methods and using expert teams. Algorithms, machine learning models, artificial neural networks, data analysis techniques, and process automation tools are used in banking intelligence. Banking uses these tools to identify fraudulent patterns and trends, predict fraudulent behavior, quickly detect fraud, and improve banking security and control systems (27-31). In banking, fraud detection is done through the use of artificial intelligence and machine learning algorithms. These algorithms can identify patterns and anomalies that suggest fraud by analyzing large volumes of data from various sources, like transaction records, customer information, and network logs, which include unauthorized access, unusual transaction patterns, and suspicious behavior. Using algorithms and computational methods; machine learning can directly extract the required information from the data for fraud detection. These methods are capable of learning information from data without the need for default equations (32, 33).

3. SUGGESTED DESIGN

The proposed plan to detect suspicious behaviors in card transactions is presented in Figure 1, based on various studies conducted in the field of credit card fraud detection and utilizing examples from related articles.

A strong and accurate model for predicting fraud is created using the combination of XGBoost and LightGBM algorithms in this model.

3. 1. Exploratory Data Analysis The fraud detection process begins with the extraction and loading of exploratory data from the bank's database. For optimal algorithm performance, this step involves transforming features, filling in empty values, removing duplicate data and noise, and using other methods such as transformation, normalization, and standardization. The data preprocessing operation is complete.

3. 2. Features Engineering Feature engineering and the opinion of expert experts are used to select important and influential data at this stage. PCA algorithms can be utilized to select the best features.

3. 3. Data Training The pre-processed data is randomly split into two training and experimental groups, with 80% belonging to training data and 20% belonging to experimental data. Then, different algorithms that were assumed to be important and reliable in previous fraud detection studies are trained in different stages using training data, so that different models of each algorithm are ready to be evaluated.

3. 4. Sampling by Smote METHOD In this step, the Smote method is used to address the problem of unsatisfied classes in the data. By generating artificial samples from existing samples, Smote can increase the number of minority class samples.

3. 5. Testing Data Different built models are used to test the data of the experimental group, and a confusion matrix of the results for each algorithm is prepared for use in step evaluating models.

3. 6. Evaluating Models The F criterion and AUC criterion are calculated for each of the confusion matrices in this step.

3. 7. Determining A Machine Learning Model First, determine the number of algorithms for which the highest F criterion was measured after reviewing the criteria calculated in step evaluating models. The number of selected algorithms is decreased based on the amount calculated for the AUC criterion. XGBoost and LightGBM algorithms were chosen after completing this stage based on the statistical population of this research and the criteria mentioned. Due to its shorter execution time compared to LightGBM, the XGBoost algorithm will be prioritized for model execution in the main stages to reduce the execution time to a suitable extent.

3. 8. New Transaction The bank's database is used to extract card-to-card transaction information for fraud detection operations at this stage.

3. 9. Preparing Data The pre-processing of the extracted information in step new transaction is done similarly to step features engineering.

3. 10. Predicting Fraud Using the Xgboost Algorithm The main fraud detection procedure commences at this point, with the use of the XGBoost algorithm. The XGBoost algorithm is a powerful machine learning algorithm that can accurately predict various data.

3. 11. Improving Fraud Detection Accuracy with The Lightgbm Algorithm In this step, the output information of step predicting fraud using the Xgboost algorithm is filtered and only the information related to the transactions that have been labeled fraudulent by the XGBoost algorithm are entered as input to the LightGBM algorithm. When it comes to dealing with large and complex datasets, the LightGBM algorithm, which is based on gradients, performs better. By using this combined algorithm, the goal is to reduce the number of false positives (FN) and increase model accuracy.

3. 12. A Caution to The Bank In the final stage, the forecast information is checked, and fraudulent transactions are notified to the bank with a warning. This process is repeated to check new transactions. By using the proposed scheme, it is possible to conduct a more detailed analysis to detect fraud in card-to-card transactions. To predict transaction information for the One of the State banks of Iran and other banks. Figure 1 shows the proposed hybrid model.

4. METHODOLOGY

The focus of this research has been on examining and discussing an important and research topic. The primary objective of this research is to investigate and analyze a particular problem or challenge and suggest innovative and appropriate solutions to resolve it. Various research methods and techniques have been employed to achieve this goal, which are described below:

The method of this research is the case study method because it specifically focuses on an Iranian state bank and an European bank.

a) The research is practical in terms of its purpose, as its results are used to inform bank managers and the task force to discover Bank Fraud and send the required reports to the Central Bank of J.A.

b) In terms of location, the research is conducted on the internet and field type. The data of the European Bank are collected through the website www.kaggle.com,

Figure 1. Suggested Design

while the data of the One of the State banks of Iran are collected through the field and legally stored in the bank's data storage unit.

c) By predicting the fraud label using transaction information from both banks within a certain period of time, the research is predictive.

d) In terms of the nature of the data, the research employs a qualitative approach. For feature engineering, this method is utilized to obtain expert opinions, views, opinions, and experiences from experts, data warehouse specialists, and individuals related to the subject under study.

4. 1. Collecting Data The first data set of the research includes credit card transactions made by a European bank for two days in 2013. The second data set includes card-to-card transactions made by the Tose'e Ta'avon bank for one month. For the Tose'e Ta'avon bank, the selected features include various variables such as age group, job, economic sector, customer membership type, terminal type, day and time and transaction amount, number and amount of daily and monthly card transactions as source and destination. if in the reviewed studies, the calculation features of the number and amount of card transactions have not been used in other time periods.

4. 2. Data Sample Quantity In the first data set, out of a total of 284,807 transactions, only 492 are fraudulent transactions and 284,315 are non-fraudulent transactions, and in the second data set, out of a total of 4,139,607 card-to-card transactions, which are related to one month, the number is 5. 161 cases have already been identified as fraudulent transactions.

4. 3. Tools For Collecting Data The information related to the first data set was received from the website www.kaggle.com and the information of the second data

set was directly compiled and engineered by the experts of the bank's data warehouse unit. Feature engineering and initial pre-processing of this educational data is also done by Oracle sql development software.

Also, the implementation of the model with machine learning algorithms and its evaluation has been done by Python coding tool and PyCharm 2021.3.3 IDE.

5. DATA ANALYSIS

In this section, the proposed design is used to analyze statistical data set information. The introduced algorithms have been used because of their power, good performance, and wide applications. In the following, the evaluation criteria of the algorithms were examined and then the algorithms were evaluated on sample data from the European Bank in order to provide a suitable solution to detect fraud in the real data of the Tose'e Ta'avon bank and an optimal process to increase its speed and accuracy.

The Xgboost Algorithm is a powerful machine learning algorithm based on gradient boosting and provides better performance than other algorithms by exploiting the power of hardware computing.

The Decision Tree (Dt) Algorithm is used for classification and regression and makes a decision by building a decision tree based on the features and conditions of the segmentation.

The Random Forest Algorithm operates based on the concept of a set of decision trees and makes decisions by combining their results.

Nearest Neighbors Algorithm is based on nearest neighbors and uses labels of neighboring samples to predict labels.

Isolation Forest Algorithm is a method to detect rare and unusual defects in data. This algorithm tries to separate defects from other data by building random trees and simulating the random process.

The Local Anomaly Factor (Lof) Algorithm uses a method to detect defects and local anomalies in the data.

Lightgbm Algorithm is a gradient boosting based machine learning algorithm developed by Microsoft. This algorithm is used for classification and regression. LightGBM is commonly used in large datasets due to its high speed and low memory consumption.

5. 1. The Criteria for Evaluation

The algorithms are evaluated against sample data from the European Bank using the specified criteria, and a suitable solution is provided to detect fraud in the data, increasing the speed and accuracy of the analysis process.

Accuracy: The ratio of the number of correctly classified data to the total number of data.

Precision: The ratio of the number of true positive data that are correctly detected to the total number of detecting positive data.

Recall: The ratio of the number of true positive data correctly recognized to the total number of true positive data.

Measurement (F1 score): F1 is a measure that combines accuracy and readability and is used to compare algorithms.

Operating characteristic curve (ROC curve): A graph that shows the ratio between the correct detection rate and the false detection rate of the algorithm.

5. 2. Comparing the Results of Different Algorithms and Selecting Suitable Algorithms

The performance of the algorithms is evaluated by dividing the dataset into two parts: training and testing. The training data set is utilized for algorithm training, while the test data set is utilized for evaluating their performance. The calculation and reporting of accuracy, recall, F-score, and ROC-AUC scores for each algorithm was done.

According to the results obtained in Table 1, the following four algorithms are selected as the best algorithms according to the record of the highest value of the F function:

XGBoostSmoted,XGBoost,LightGBM,Smoted LightGBM

In the next step, the following two algorithms are selected according to the record of the highest ROC-AUC criterion: Smoted XGBoost, Smoted LightGBM.

Finally, considering the higher processing time of the Smoted LightGBM algorithm and the large number of input data, we arrange the algorithms in such a way that the data processing takes place in the following two steps:

TABLE 1. Evaluation results with different methods in the European Bank

Algorithm	Smote	F Score	Time training (s)	ROC-AUC
XGBoost	NO	0.9996	28.60	0.8928
XGBoost	YES	0.9996	91.16	0.9285
Decision Tree	NO	0.9994	8.76	0.8928
Decision Tree	YES	0.9982	110.83	0.8027
Random Forest	NO	0.9996	2683.57	0.8928
Random Forest	YES	0.9995	5135.88	0.9234
KNN	NO	0.9984	0.07	0.6570
KNN	YES	0.9708	0.19	0.7867
Isolation Forest	NO	0.9510	4.804	0.9092
Isolation Forest	YES	0.9924	8.407	0.6295
LOF	NO	0.9442	54.466	0.7378
LOF	YES	0.9380	244.241	0.6379
LightGBM	NO	0.9998	131.685	0.9030
LightGBM	YES	0.9998	343.914	0.9183

First, the data is processed by the XGBoost algorithm and fraud label prediction is done.

In this step, the output of the previous step is filtered, only the data that includes the label Class=1 are entered into the Smoted LightGBM algorithm as input, and these data are re-predicted as primary data with the corresponding Class.

Once the data has been processed, it's crucial to pay attention to these points:

- Due to the greatly reduced amount of data in the input of the second stage, the prediction operation can be performed at a higher speed in the second stage.
- FP cases pertain to transactions that are not fraudulent, but the first algorithm (XGBoost) recognizes them as fraud, and the second algorithm (LightGBM) significantly decreases the model's accuracy.

Figure 2's ROC diagram shows that the two selected algorithms are better than the other reviewed algorithms. Two algorithms, XGBoost and LightGBM, are chosen to optimize the model and detect fraud in card transaction information in the European Bank dataset.

5. 2. Testing the Model and Its Results on the Real Data of the Tose'e Ta'avon Bank First, using the XGBoost algorithm, the data of Tose'e Ta'avon bank is divided into two parts, training and testing, in such a way that the training data includes a small portion of the whole data. The Smote algorithm is used to balance the training data since the data with label 1 is very limited and much less than the data with label 0, and the data set is unbalanced.

Because the prediction is based on the type of fraud detection, the goal is to first increase the number of fraud cases correctly detected and then decrease the number of non-fraud cases that are falsely detected to increase accuracy. The training data is used for supervised learning, and then the entire bank transaction information is tested. The confusion matrix of Figure 3 is obtained as a result. According to the analysis and evaluation results of the XGBoost hybrid algorithm using Smote, it can be seen that this algorithm performed very well with 99.76% accuracy. The confusion matrix shows that out of a total of 4,144,892 samples, approximately 4,139,607 were correctly identified as negative samples, and only 8,285 were identified as false positive samples. Also, the accuracy of positive and negative predictions is 99.96% and 29.64%, respectively. The recall rates are 99.80% and 67.64%, and the F score is 0.9988 for negative samples and 0.4122 for positive samples. Also, the area under the ROC-AUC chart equal to 0.8372 shows that the algorithm has a good ability to distinguish between the two categories. The XGBoost algorithm's performance has been improved by the use of the Smote technique, and the processing time was approximately 388.23 seconds. Equation 1 is the equivalent of the total number of fraudulent transactions.

$$\text{Count}([\text{Class}] == 1) = \text{TP} + \text{FP} = 3491 + 1670 = 5161 \quad (1)$$

The total number of cases was 5,161, but only 3,491 were correctly identified. But the number of 8,285 cases was also wrongly labeled as fraud, which is considered a new data set to solve this issue in the continuation of the transactions in relation 2.

$$\text{TP} + \text{FN} = 3.491 + 8.285 = 11.776 \quad (2)$$

The number of 11,776 transactions is entered as input to the LightGBM algorithm, and again the supervised learning steps are performed on the training data of the filtered dataset, and then data testing is performed on all 11,776 transactions, and finally the results are according to the matrix The confusion of Figure 4 is obtained.

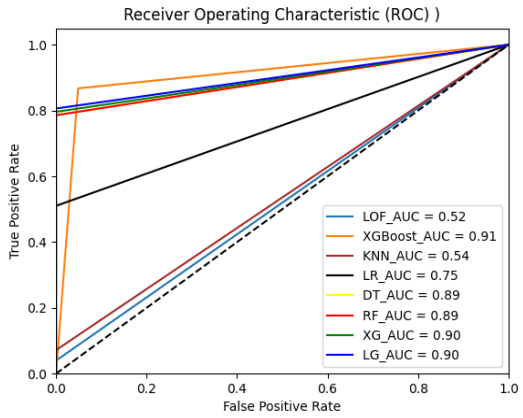


Figure 2. ROC graph for different algorithms without using Smote technique

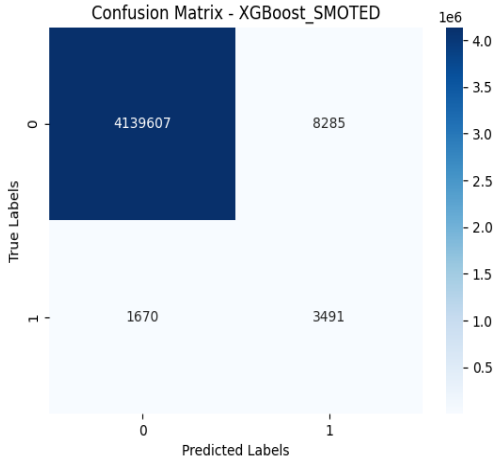


Figure 3. Confusion matrix of XGBoost algorithm with Smote on real data of Tose'e ta'avon bank

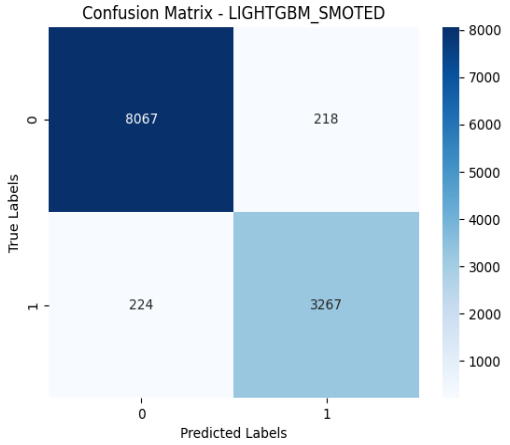


Figure 4. Confusion matrix of LightGBM algorithm with Smote on real data of Tose'e ta'avon bank after filtering

The combined algorithm's analysis and evaluation results indicate that it has a good performance with a 96.25% accuracy. The confusion matrix indicates that among 8,776 samples, approximately 8,067 were correctly identified as negative samples, while only 218 were identified as false positive samples. Also, the accuracy of positive and negative predictions is 97.30% and 93.74%, respectively. The recall results are 97.37% and 93.58%, with the F score being 0.9733 for negative samples and 0.9366 for positive samples. The algorithm's ability to distinguish between the two categories is demonstrated by the 0.9548 area under the ROC-AUC chart. The algorithm's performance on the test data is demonstrated by the ROC-AUC score of 0.9562 on the test set.

According to equation 3, it is evident that the model decreases the items related to FN by keeping TP and enhances the accuracy of the output.

$$\begin{aligned} &TN + TP + FP + FN = 8.067 + 3.267 + 224 + 218 = 11.776 \\ &FN1 = 8.285, FN2 = 218 \\ &TP1 = 3491, TP2 = 3267 \end{aligned} \quad (3)$$

Therefore, the model is also optimized by selecting two algorithms XGBoost and LightGBM to detect fraud in card transaction information in the Tose'e Ta'avon bank dataset.

6. CONCLUSION

According to comprehensive analyses and tests, the proposed model was developed to detect fraud in the transaction information of the Tose'e Ta'avon bank, using XGBoost and LightGBM algorithms. The objective of this algorithm combination is to detect defects and anomalies in data with high speed and accuracy. The experiments demonstrate that this model with high accuracy can correctly detect defects and provide reliable information about the data's state. Using the existing knowledge and experience in the field of data analysis and machine learning, it is certain that this model with the combination of XGBoost and LightGBM has the ability to detect fraud in the information of The Tose'e Ta'avon bank well and can be used as a powerful tool in detecting fraud. In this research, an advanced method for detecting fraud in transactions was presented. There are two main steps in this method. The XGBoost algorithm is used to identify frauds by entering transaction information after preprocessing. Only the transactions that received the fraud label in the first step are included after filtering the output of this algorithm. To enhance fraud detection accuracy, the filtered information is fed into the LightGBM algorithm in the second step. The accuracy of fraud detection is significantly increased by this step. The results show that by combining XGBoost and LightGBM algorithms with two stages of fraud detection, the speed and accuracy of fraud detection are significantly increased. This method can be used in banking and financial transaction systems that face various types of fraud. The proposed method in the current research provides a reliable and accurate solution to detect fraud in Tose'e Ta'avon bank transactions. This method can significantly improve the speed and accuracy of fraud detection and can be used in financial and banking transaction systems.

7. REFERENCES

1. Merryta D, Tuga M. Artificial Intelligence Model as an Early Warning System for Fraudulent Transactions in Mobile Banking. ICIC Express Letters Part B: Applications. 2023;14(07):747. https://doi.org/10.24507/icicelb.14.07.747
2. Madhuri TS, Babu ER, Uma B, Lakshmi BM. Big-data driven approaches in materials science for real-time detection and prevention of fraud. Materials Today: Proceedings. 2023;81:969-76. https://doi.org/10.1016/j.matpr.2021.04.3232214-7853/_
3. Mytnyk B, Tkachyk O, Shakhovska N, Fedushko S, Syerov Y. Application of Artificial Intelligence for Fraudulent Banking Operations Recognition. Big Data and Cognitive Computing. 2023;7(2):93. https://doi.org/10.3390/bdcc7020093
4. Ogundokun RO, Misra S, Ogundokun OE, Oluranti J, Maskeliunas R, editors. Machine learning classification based techniques for fraud discovery in credit card datasets. Applied Informatics: Fourth International Conference, ICAI 2021, Buenos Aires, Argentina, October 28–30, 2021, Proceedings 4; 2021: Springer.
5. Seeja K, Zareapoor M. Fraudminer: A novel credit card fraud detection model based on frequent itemset mining. The Scientific World Journal. 2014;2014. http://dx.doi.org/10.1155/2014/252797
6. Padhi B, Chakravarty S, Biswal B, editors. Anonymized credit card transaction using machine learning techniques. Advances in Intelligent Computing and Communication: Proceedings of ICAC 2019; 2020: Springer.
7. Moradi R, Hamidi H. A New Mechanism for Detecting Shilling Attacks in Recommender Systems Based on Social Network

Analysis and Gaussian Rough Neural Network with Emotional Learning. International Journal of Engineering, Transactions B: Application. 2023;36(2):321-34. https://doi.org/10.5829/ije.2023.36.02b.12

8. Sharma D, Kang SS, editors. Hybrid model for detection of frauds in credit cards. 2022 4th International Conference on Advances in Computing, Communication Control and Networking (ICAC3N); 2022: IEEE.
9. Zhang Y, Chen X, Li J, Wong DS, Li H, You I. Ensuring attribute privacy protection and fast decryption for outsourced data security in mobile cloud computing. Information Sciences. 2017;379:42-61. https://doi.org/10.1016/j.ins.2016.04.015
10. Timothy DP, Santra AK, editors. A hybrid cryptography algorithm for cloud computing security. 2017 International conference on microelectronic devices, circuits and systems (ICMDCS); 2017: IEEE.
11. Hashemi SK, Mirtaheri SL, Greco S. Fraud Detection in Banking Data by Machine Learning Techniques. IEEE Access. 2022;11:3034-43.
12. Nkomo BK, Breetzke T, editors. A conceptual model for the use of artificial intelligence for credit card fraud detection in banks. 2020 Conference on Information Communications Technology and Society (ICTAS); 2020: IEEE.
13. Pham VVH, Liu X, Zheng X, Fu M, Deshpande SV, Xia W, et al., editors. PaaS-black or white: an investigation into software development model for building retail industry SaaS. 2017 IEEE/ACM 39th International Conference on Software Engineering Companion (ICSE-C); 2017: IEEE.
14. Aljawarneh S. Cloud security engineering concept and vision: Concept and vision. Cyber security and threats: Concepts, methodologies, tools, and applications: IGI Global; 2018. p. 93-101.
15. Khan N, Al-Yasiri A. Cloud security threats and techniques to strengthen cloud computing adoption framework. Cyber security and threats: Concepts, methodologies, tools, and applications: IGI Global; 2018. p. 268-85.
16. Khosravi S, Kargari M, Teimourpour B, Eshghi A, Aliabdi A, editors. Using Supervised Machine Learning Approaches To Detect Fraud In The Banking Transaction Network. 2023 9th International Conference on Web Research (ICWR); 2023: IEEE.
17. Balagolla E, Fernando W, Rathnayake R, Wijesekera M, Senarathne A, Abeywardhana K, editors. Credit card fraud prevention using blockchain. 2021 6th international conference for Convergence in Technology (I2CT); 2021: IEEE.
18. Bahrami L, Safaie N, Hamidi H. 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. 2021;34(12):2624-35. https://doi.org/10.5829/ije.2021.34.12c.07
19. Kirar JS, Kumar D, Chatterjee D, Patel PS, Yadav SN, editors. Exploratory Data Analysis for Credit Card Fraud Detection. 2021 International Conference on Computational Performance Evaluation (ComPE); 2021: IEEE.
20. Alghushairy O, Alsini R, Ma X, editors. An Efficient Local Outlier Factor for Data Stream Processing: A Case Study. 2020 International Conference on Computational Science and Computational Intelligence (CSCI); 2020: IEEE.
21. Hamidi H, Rafebakhsh M. Analyzing factors influencing mobile social media marketing acceptance among customers. International Journal of Engineering, Transactions C: Aspects. 2022;35(6):1209-16. https://doi.org/10.5829/ije.2022.35.06c.13
22. Hamidi H, Seyed Lotfali S. Analysis of role of cloud computing in providing internet banking services: Case study bank melli iran. International Journal of Engineering, Transactions B: Application. 2022;35(5):1082-8. https://doi.org/10.5829/ije.2022.35.05b.23
23. Daliri S. Using harmony search algorithm in neural networks to improve fraud detection in banking system. Computational Intelligence and Neuroscience. 2020;2020. https://doi.org/10.1155/2020/6503459
24. Esmail FS, Alsheref FK, Aboutabl AE. Review of Loan Fraud Detection Process in the Banking Sector Using Data Mining Techniques. International journal of electrical and computer engineering systems. 2023;14(2):229-39. https://doi.org/10.32985/ijeces.14.2.12
25. Handa A, Dhawan Y, Semwal P. Hybrid analysis on credit card fraud detection using machine learning techniques. Handbook of Big Data Analytics and Forensics. 2022:223-38. https://doi.org/10.1007/978-3-030-74753-4_15
26. Hamidi H. A combined fuzzy method for evaluating criteria in enterprise resource planning implementation. Intelligent systems: Concepts, methodologies, tools, and applications: IGI Global; 2018. p. 639-70.
27. Nilchi AN, Vafaei A, Hamidi H, editors. Evaluation of security and fault tolerance in mobile agents. 2008 5th IFIP International Conference on Wireless and Optical Communications Networks (WOCN'08); 2008: IEEE. 10.1109/WOCN.2008.4542509
28. Parekh P, Rana C, Nalawade K, Dholay S, editors. Credit Card Fraud Detection with Resampling Techniques. 2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT); 2021: IEEE. 10.1109/ICCCNT51525.2021.9579915
29. Patil S, Nemade V, Soni PK. Predictive modelling for credit card fraud detection using data analytics. Procedia computer science. 2018;132:385-95. https://doi.org/10.1016/j.procs.2018.05.199
30. Sharma U, Sharma M, Rana A, editors. Experimental Analysis of Anomaly Detection Algorithms on Banking data. 2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO); 2021: IEEE.
31. Rambola R, Varshney P, Vishwakarma P, editors. Data mining techniques for fraud detection in banking sector. 2018 4th International Conference on Computing Communication and Automation (ICCCA); 2018: IEEE.
32. Hamidi H, Vafaei A, Monadjemi SA. Evaluation and checkpointing of fault tolerant mobile agents execution in distributed systems. Journal of Networks. 2010;5(7):800.
33. Hamidi H, Moradi S. Analysis of consideration of security parameters by vendors on trust and customer satisfaction in e-commerce. Journal of Global Information Management (JGIM). 2017;25(4):32-45. 10.4018/JGIM.2017100103

Persian Abstract

چکیده

در سال‌های اخیر، با افزایش دسترسی به داده‌های مشتریان و توانایی‌های پیشرفته تحلیل داده‌ها با استفاده از روش‌های هوشمند، برای تحلیل رفتار مشتریان اقدامات مختلفی صورت گرفته است. یکی از این اقدامات، استفاده از سیستم‌های هوشمند برای کشف تقلب در بانکداری است. تقلبات بانکی در حال حاضر گستره وسیعی دارند و باعث آسیب‌های مالی و غیرمالی جدیدی به بانک‌ها و مشتریان آن‌ها شده‌اند. با توجه به اهمیت موضوع، در این تحقیق یک مدل هوشمند برای کشف تقلب در بانکداری طراحی شده است. پس از استفاده از ابزارهای هوشمندسازی برای بررسی الگوریتم‌های مختلف یادگیری ماشین ، دو الگوریتم XGBoost و LightGBM به دلیل برتری معیارهای F و ROC در مدل مورد نظر انتخاب شدند. این الگوریتم‌ها به صورت مرحله‌ای در آزمایشات نهایی استفاده شدند تا همزمان با دقت بالا، تعداد نمونه‌های نادرست با برچسب تقلب (FP) را کاهش دهند. این مدل با استفاده از داده‌های واقعی یک بانک دولتی آزمایش شده و نتایج بسیار قابل قبولی در تشخیص تقلب در تراکنش‌های کارت به کارت ارائه می‌دهد. این مدل می‌تواند بهبود چشمگیری را در امنیت سیستم بانکی فراهم کند و به عنوان ابزاری موثر در کاهش جرایم مالی استفاده شود.