engineering proceedings

MDPI

Proceeding Paper

Detection of Bank Transaction Fraud Using Machine Learning †

Muhammad Sami [1,*], Azka Mir [1] and Gina Purnama Insany [2]

[1] Department of Software Engineering, University of Sialkot, Sialkot 51310, Pakistan; azka.mir@uskt.edu.pk
[2] Department of Informatics Engineering, Faculty of Engineering, Nusa Putra University, Sukabumi 43152, West Java, Indonesia; gina.purnama@nusaputra.ac.id
* Correspondence: 21101001-075@uskt.edu.pk
† Presented at the 7th International Global Conference Series on ICT Integration in Technical Education & Smart Society, Aizuwakamatsu City, Japan, 20–26 January 2025.

Abstract

Bank transaction fraud detection has emerged as an important area of research in the economic sector, driven by the developing sophistication of fraudulent activities and the considerable economic losses they entail. This paper reviews numerous methodologies and technologies employed in the real-time identification and mitigation of fraudulent transactions, including traditional statistical techniques, machine learning algorithms and advanced artificial intelligence strategies. It enhances the need to combine anomaly detection structures with behavioral analytics to enhance detection accuracy while addressing challenges like data privacy, the need to balance false positives and negatives and the need for adaptive systems. By evaluating the most recent developments and case studies, this study provides a comprehensive assessment of what is happening in bank transaction fraud detection and presents future directions for enhancing safety features.

Keywords: fraud detection; bank transactions; machine learning; anomaly detection; behavioral analytics

1. Introduction

The effect of rapid growth in the usage of online banking is evident in the increase in the volume of noncash transactions around the world [1]—the growth in the volume of cashless transaction was 10.1% in 2016, increasing the number to 482.6 billion; projections post 2021 indicate a CAGR of 12.7% [1]. But while digital banking might be flourishing, so too is online banking fraud; such fraud in the UK cost GBP 121.4 million in 2017, up from GBP 63.7 million in 2010 [2].

These manual processes of banking fraud hinder new strategies employed by corporations aimed at combating such nefarious activities. Work is being conducted on certain rule-based fraud detection systems, but updating them often proves troublesome. However, there has been an increase in the usage of machine learning to flag online banking fraud [3]. Most current works employ the non-sequential transaction model or assumptions which are quite restrictive [4].

The first classifier worked within the boundaries of individual transaction sequences by refocusing data points keeping an eye on appropriate ones [5]. This solution considers the problem of online payment fraud as a classification problem, turning it into a real-time transaction risk assessment. The hierarchical attention strategy allows us to understand the wider context while maintaining accuracy in the detection of specific transactions [6].

Academic Editors: Debopriyo Roy, George F. Fragulis and Peter Ilic

Published: 28 August 2025

Citation: Sami, M.; Mir, A.; Insany, G.P. Detection of Bank Transaction Fraud Using Machine Learning. *Eng. Proc.* **2025**, *107*, 34. https://doi.org/10.3390/engproc2025107034

Our study has two main contributions: it proposes an attention network that incorporates transactional information into global fraudulence decisions, and it guarantees that the rationale behind the decisions is readable by the users. Validation on a reasonably large sample of real bank transactions has indicated its robustness in fraud detection over previously employed methods, estimating trends and outliers and reducing the number of false positives to a minimum [7].

2. Literature Review

The replacement of rule-based applications with machine learning (ML) and deep learning (DL) algorithms has contributed markedly to the advancement of fraud detection capability by allowing systems to pick up hidden patterns that would be difficult for other methods to recognize [1]. Architectures have been proposed—for example, credit card fraud detection systems that employ neural networks—that have shown the ability of DL to classify various kinds of transactions to keep up with the changing nature of fraud [2]. The CoDetect algorithm has demonstrated its capability in the scaling and efficient processing of vast quantities of data, thus demonstrating the significance of rapid algorithms for real-world applications [3]. In the same way, the AIS-based fraud detection model has improved the accuracy and reduced the cost of the detection of fraud, which calls for the adoption of new ideas to address the increasing levels of fraudulent activities [4].

In one study, the model interpretability was improved by the random forest algorithm, which utilized decision trees from a random selection of a dataset to yield results that demonstrate the control of essential features [5]. In the same sense, a review on cutting-edge techniques indicates that transaction aggregation and feature manipulation are important for enhancing model accuracy, as the features define how well the model performs [6]. Workarounds, such as feature engineering and modification—with the aim of detecting minority-class problems including fraud, which represent a considerable challenge—have been employed to lessen the effects of imbalanced datasets [7]. Additionally, fraud detection capabilities have been improved by data mining methods because they are able to detect hidden patterns in transaction data [8].

Deep learning models show incredible adaptability in dealing with new fraud techniques, and their detection rates are improving over time. Their ability to adapt to new threats highlights their importance, but strong adversarial defenses remain critical for reducing vulnerabilities against adversarial actors [9,10]. Studies on artificial intelligence (AI) and machine learning (ML) in fraud detection highlight their growing significance in the business, providing standards to guide the implementation of scalable and effective solutions [11]. Also, future technologies like quantum computing have the potential to transform this field by enhancing the accuracy of existing models, leading to a new frontier in fraud detection research [12]. The current research improves these foundations by addressing gaps in data management, performance metrics and usability by applying an integrated ML approach [13].

3. Methodology

3.1. Data Collection and Processing

The dataset used in this study contains 2512 records including 16 features, providing valuable information on transaction behaviors [14]. These features include Transaction Amount, Transaction Type, Customer Age, Customer Occupation and Account Balance, among others, contributing to a establishing a complete understanding of transaction patterns and user profiles. Several preparation processes were performed on the data before it was analyzed. Categorical information like Transaction Type, Location, Channel and Customer Occupation were encoded with Label Encoder, allowing its numerical repre-

sentation. To retain information detail, one-hot encoding was used for many attributes. Standard Scaler was used to normalize numerical features like Transaction Amount, Transaction Duration, and Account Balance, which ensured feature consistency and enhanced algorithmic performance [15]. Date-related features like Transaction Date and Previous Transaction Date were converted into datetime objects, which enable the gathering of additional time-related data such as transaction interval and time. Missing values were handled by replacing categorical features with "Unknown" and numerical features with their median value. Outlier analysis with z-scores guaranteed that the data were handled correctly. These methods ensured that the dataset was valid and ready for analysis.

3.2. Splitting the Dataset

The dataset was split into two sets, training (80%) and testing (20%), to evaluate model performance. Stratified sampling was used to maintain the distribution of transaction types in both datasets, reducing unfairness. Class imbalance was analyzed, and techniques like SMOTE were used if needed.

3.3. Feature Selection

The most important factors were selected using a Random Forest model for feature selection. Attributes like Transaction Amount, Account Balance and Transaction Type were shown to be important predictors. Correlation analysis showed dependence between features, and duplicate variables were eliminated to improve model accuracy.

3.4. Model Development

The following ML algorithms were used:

1. KKN: For KNN, we adopted k values of 1, 3, 5 and 7. This basic technique showed the differences in performance based on neighborhood size.
2. Random Forest: The ensemble learning model Random Forest was fine-tuned using GridSearchCV to optimize parameters such as the number of estimators and maximum depth. It is capable of handling feature importance ranking and is robust against overfitting.
3. Gradient Boosting: The Random Forest ensemble learning model was improved using GridSearchCV to optimize parameters like estimate number and maximum depth. It is capable of handling feature priority and avoids overfitting.
4. Ensemble Method: Gradient Boosting can be used to effectively model non-linear relationships. The model's iterative learning method allowed it to fix errors in an orderly way, leading to excellent prediction accuracy.

4. Results and Discussion

4.1. Model Performance

The analysis evaluates a range of parameters for each of the models investigated, including accuracy, precision and recall. The results showed that Gradient Boosting and Random Forest outperformed the other models, showing their ability to deal with non-linear relationships and feature interactions. KNN also scored well but was still susceptible to noisy input. Figure 1 shows the accuracy values visualization.

The Voting Classifier delivered the best overall performance, benefiting from the combined strengths of each individual model.

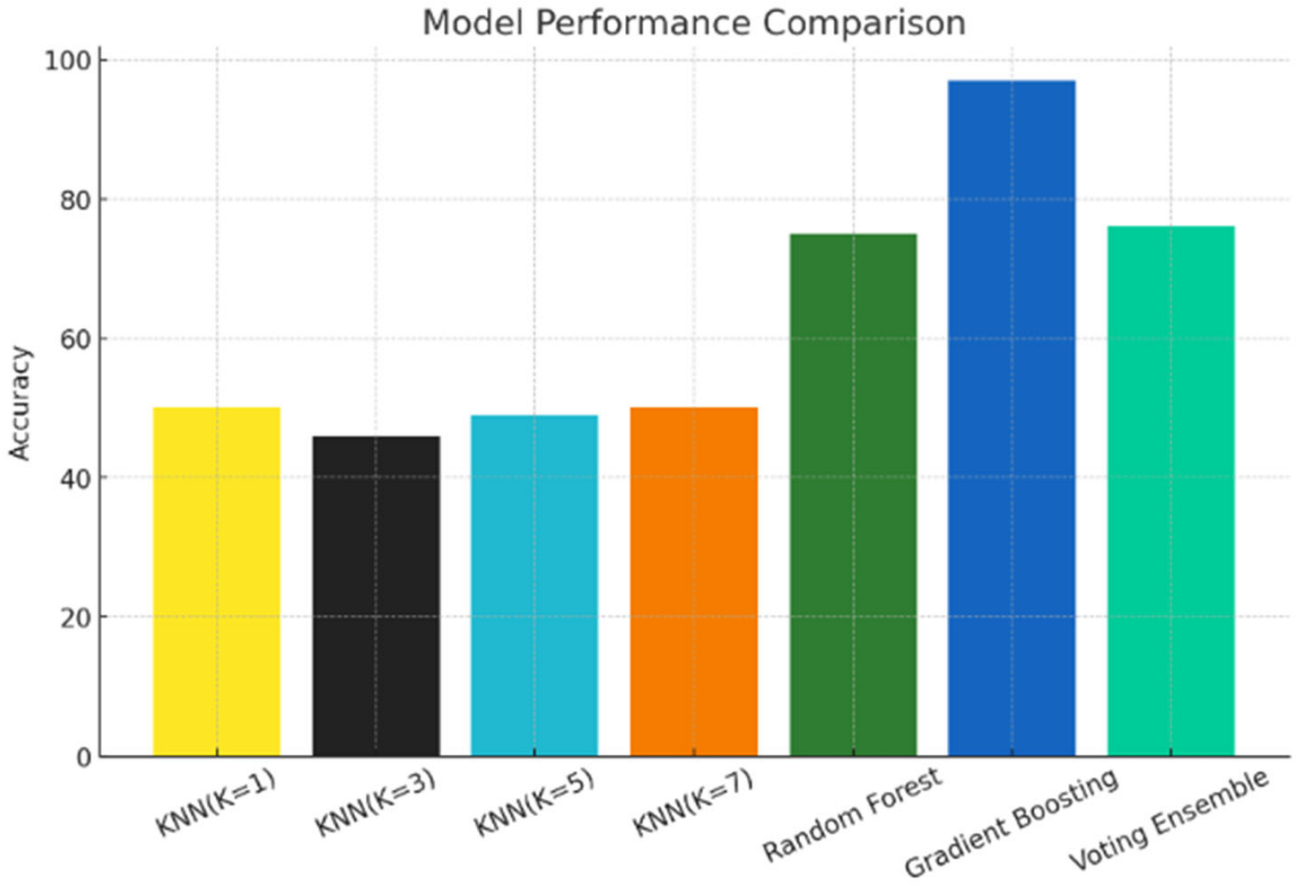

Figure 1. Accuracy scores of all models.

4.2. Feature Importance

The Random Forest analysis showed that transaction amount, transaction duration and account balance were the most important features influencing fraud detection. These features focus on importance of monitoring unusual transaction patterns, unusual timing and sudden changes in account balances, which may be indicators of a transaction fraud. Table 1 shows the final evaluation results.

Table 1. Outcomes of every algorithm utilized in this study.

Model	Accuracy	Precision	Recall	Confusion Matrix
KNN (k = 1)	50.80%	53.56%	48.48%	[127, 111], [136, 128]
KNN (k = 3)	46.81%	44.66%	48.95%	[118, 122], [145, 117]
KNN (k = 5)	49.60%	47.43%	53.97%	[120, 110], [143, 129]
KNN (k = 7)	50.60%	48.33%	54.39%	[124, 109], [139, 130]
Random Forest	75.75%	40.00%	75.75%	[5, 109], [13, 376]
Gradient Boosting	97.61%	45.53%	47.50%	[1, 104], [8, 381]
Voting Ensemble (Soft)	76.74%	64.32%	76.74%	[1, 113], [4, 385]

5. Conclusions and Future Work

This study has made significant progress in developing a machine learning (ML) model which is capable of detecting illegal bank transactions with high accuracy and robustness. We suggested that machine learning (ML) algorithms can identify fraudulent transaction data with accurate training and evaluation. Among the models evaluated, Gradient Boosting and the Voting Classifier exhibited exceptional predictive performance.

But further optimization is required to improve their sensitivity and ability to deal with class imbalance, providing accurate identification across a wide range of fraud cases.

For future studies, we suggest using different combinations of models and also focusing directly on CatBoost by changing more hyperparameters than specifically those affecting the number of trees. Also, due to devices restrictions in this investigation, using stronger and better technology may produce enhanced outcomes that can be compared to the results obtained in this study.

Our findings have wide-ranging implications that could enhance bank security and prevent fraud. This study provides the groundwork for enhanced and scalable methods to identify fraud in the banking industry with accurate, data-driven results.

Author Contributions: Conceptualization, M.S.; Methodology, M.S. and A.M.; Formal Analysis, M.S.; Data Curation. M.S.; Writing Original Draft Preparation, M.S.; Project Administration, M.S.; Software, A.M.; Investigation, A.M. and G.P.I.; Visualization, A.M.; Validation. G.P.I.; Resources, G.P.I.; Writing Review and Editing, G.P.I.; Supervision, G.P.I. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data that support the findings of this study are available from the corresponding author upon reasonable request.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Alonge, E.O.; Eyo-Udo, N.L.; Ubanadu, B.C.; Daraojimba, A.I.; Balogun, E.D.; Ogunsola, K.O. Enhancing data security with machine learning: A study on fraud detection algorithms. *J. Data Secur. Fraud. Prev.* **2021**, *7*, 105–118. [CrossRef]
2. Fu, K.; Cheng, D.; Tu, Y.; Zhang, L. Credit card fraud detection using convolutional neural networks. In *Lecture Notes in Computer Science, Proceedings of the International Conference on Neural Information Processing, Kyoto, Japan, 16–21 October 2016*; Springer: Cham, Switzerland, 2016; pp. 483–490.
3. Banerjee, R.; Bourla, G.; Chen, S.; Kashyap, M.; Purohit, S. Comparative analysis of machine learning algorithms through credit card fraud detection. In Proceedings of the 2018 IEEE MIT Undergraduate Research Technology Conference (URTC), Cambridge, MA, USA, 5–7 October 2018; pp. 1–4.
4. Alhabib, A.A.; Alasiri, A.F.; Alharbi, M.B.; Ahmad, S.; Eljialy, A.E.M. Credit Card Fraud Detection Using Random Forest and K-Nearest Neighbors (KNN) Algorithms. In Proceedings of the International Conference on Cognitive Computing and Cyber Physical Systems, Delhi, India, 1–2 December 2023; pp. 383–395.
5. Kumar, Y.; Saini, S.; Payal, R. Comparative analysis for fraud detection using logistic regression, random forest and support vector machine. *SSRN Electron. J.* **2020**, *7*, 726–731. [CrossRef]
6. Olszewski, D. Fraud detection using self-organizing map visualizing the user profiles. *Knowl.-Based Syst.* **2014**, *70*, 324–334. [CrossRef]
7. Kültür, Y.; Çağlayan, M.U. Hybrid approaches for detecting credit card fraud. *Expert Syst.* **2016**, *34*, e12191. [CrossRef]
8. Nguyen, H.T.; Liang, P.J.; Akoglu, L. Anomaly detection in large labeled multi-graph databases. *arXiv* **2020**, arXiv:2010.03600.
9. Chen, Z.; Soliman, W.M.; Nazir, A.; Shorfuzzaman, M. Variational autoencoders and wasserstein generative adversarial networks for improving the anti-money laundering process. *IEEE Access* **2021**, *9*, 83762–83785. [CrossRef]
10. Hancock, J.T.; Khoshgoftaar, T.M. Gradient boosted decision tree algorithms for medicare fraud detection. *SN Comput. Sci.* **2021**, *2*, 268. [CrossRef]
11. Owolafe, O.; Ogunrinde, O.B.; Thompson, A.F.B. A long short term memory model for credit card fraud detection. In *Artificial Intelligence for Cyber Security: Methods, Issues and Possible Horizons or Opportunities*; Springer: Cham, Switzerland, 2021; pp. 369–391.
12. Maftoun, M.; Ranjbar, A.M.; Ghavitan, H.; Khademi, M. Attention-Based Deep Learning Models for Fraud Detection in Imbalanced Transaction Datasets. In Proceedings of the 2025 11th International Conference on Web Research (ICWR), Tehran, Iran, 16–17 April 2025; pp. 130–136.

13. Diwaker, C.; Tomar, P.; Solanki, A.; Nayyar, A.; Jhanjhi, N.Z.; Abdullah, A.; Supramaniam, M.A. A New Model for Predicting Component Based Software Reliability Using Soft Computing. *IEEE Access* **2019**, *7*, 147191–147203. [CrossRef]
14. Kok, S.H.; Abdullah, A.; Jhanjhi, N.Z.; Supramaniam, M.A. A Review of Intrusion Detection System Using Machine Learning Approach. *Int. J. Eng. Res. Technol.* **2019**, *12*, 8–15.
15. Ahmed, S.; Hossain, M.A.; Bhuiyan, M.M.I.; Ray, S.K. A Comparative Study of Machine Learning Algorithms to Predict Road Accident Severity. In Proceedings of the 2021 20th International Conference on Ubiquitous Computing and Communications (IUCC/CIT/DSCI/SmartCNS), Virtual, 20–22 December 2021; pp. 390–397. [CrossRef]