

# Analysis of Fraud Detection Solutions Using Machine Learning (DSR Approach)

**Vakil. Seyed Mohammad Reza**

PhD, IT Management, Department of Industrial Management, Faculty of Management, Central Tehran branch, Islamic Azad University, Tehran, Iran

**Ahmadirad. Javad**

MSc Accounting, Department of Management and Accounting, Faculty of Farabi Pardis, University of Tehran, Qom, Iran

## Abstract

The research aims to identify the problems and details of fraud detection methods in bank transactions using machine algorithms and to provide solutions in this field. Qualitative research is conducted for this aim, and the main problems are identified by reviewing previous research. Then, solutions are presented using the Design Science Research Methodology (DSR). The main topics identified from previous research include Data limitation, labeled data, Discovering new fraud patterns, Bias and Costs, and responsibility for false prediction. The proposed research model has been designed using results from previous studies and experts' opinions in this field. Using both supervised and unsupervised algorithms in the transaction registration process, labeling data based on discovered patterns, obtaining customer confirmation in cases where the system detects fraud, training, and continuous improvement of learning models using the generated data online are among the solutions of the suggested model. Also, it is suggested that the issue of reducing the error of false harmful data in the fraud detection process be investigated in future research.

**Keywords:** Fraud Detection, Machine Learning, Bank Transaction, Data Analysis, DSR Methodology

## 1. Introduction

Today, the growth of the banking network and the increasing number of transactions, especially online transactions, are consistently accompanied by the challenge of fraud. Fraud, in its simplest definition, refers to seeking profit and exploitation through unethical and criminal methods. Conventional approaches to fraud detection, which primarily rely on rule-based algorithms, have demonstrated their inability to adapt to the ever-changing nature of fraudulent practices [1].

Therefore, with its diverse data analysis techniques, artificial intelligence has become a practical tool in both the prevention and detection phases of fraud. Machine learning models are among the AI tools used for operational tasks in this field, as well as data processing, including supervised and unsupervised learning methods.

In research related to fraud detection, various techniques have been examined based on available data, primarily within supervised systems. However, the main challenge lies in Raghavan's definition of fraud [2], which highlights two key characteristics: dynamism and the lack of a fixed pattern.

These concepts emphasize the innovation and dynamic nature of fraud patterns, suggesting that fraudsters constantly seek methods that have not been used before, making detection more challenging. Consequently, this underscores the importance of selecting appropriate models and designing effective fraud detection systems.

Based on studies conducted in the field of fraud detection in banking transactions, model selection is crucial from several aspects:

- **Pattern Recognition Process:** Given the variable and dynamic nature of fraud in transactions, techniques that are continuously learning and capable of generalizing and identifying new features through behavioral analysis are more successful.
- **Process Execution Time:** Since a significant portion of online transactions are conducted in real-time, fraud prevention techniques are more effective if they can identify fraudulent behaviors with new patterns based on learned patterns, provide warnings or prevent fraudulent actions, and integrate these new patterns into the retraining process.
- **Processing Cost:** Considering the substantial volume of banking transactions and the high computational cost of implementing machine learning models, it is essential to select the most cost-effective technique based on the specific operation.

Therefore, this study aims to identify the challenges of fraud detection techniques in banking transactions highlighted in previous research and ultimately propose an optimal solution considering the identified issues and limitations.

## 2. Literature Review and Theoretical Background

**Fraud:** This term has different definitions depending on the context in which it is used. However, the common concept across all contexts is the deceptive nature of the act. Specifically, in the financial domain, it can be defined as a wrongful and criminal act of deception aimed at personal gain [3]. The consequences of such fraudulent activities deeply impact the financial ecosystem, leading to significant economic losses and eroding consumer trust [4].

**Types of Fraud:** Fraud in the banking system occurs in various forms, such as identity theft, phishing or online fraud, fraud in online transactions, and fraud related to bank cards and checks. Sometimes, a fraud process may involve a combination of these types. However, the focus of this research is on online transaction fraud.

**Fraud Detection:** A system that helps identify and provide quick alerts when fraudulent transactions are formed [5]. These systems primarily focus on identifying customer behavior to detect unusual activities [6]. If fraud can be detected before it occurs, this mechanism is referred to as fraud prevention in the initial stages of formation.

**Artificial Intelligence (AI):** Artificial Intelligence is a collection of technologies, processes, and approaches vital for the current and future growth of a comprehensive and vital economy [7]. AI enables a system to demonstrate capabilities similar to human intelligence, including understanding, reasoning, learning, interacting, and more [8].

Artificial Intelligence and Fraud Detection: In fraud detection, AI-based systems are significantly more effective at identifying fraudulent activities than conventional techniques. AI technologies enhance fraud detection processes' accuracy, speed, and scalability, thereby reducing financial losses and minimizing the negative impacts on customers.

Machine Learning Models: Machine learning models are among the tools of artificial intelligence. They can identify fraudulent patterns that have never been observed before. These models learn from past data and adapt to evolving fraud strategies [9].

Supervised learning models (algorithms), such as decision trees and random forests, are widely used to identify fraudulent transactions by learning from historical data. Unsupervised learning methods, including clustering and anomaly detection, are employed to identify new fraud patterns outside the established recognition boundaries [10].

Some of the most commonly used machine learning models for fraud detection are shown in Table 1.

**Table 1: Machine Learning Models for Fraud Detection**

Model Name	Short Description	Supervised/Unsupervised
<b>Support Vector Machines (SVM)</b>	A classification method used for linear classification.	Supervised
<b>Hidden Markov Model (HMM)</b>	A dual random process used to model more complex random processes.	Unsupervised
<b>K-Nearest Neighbors (KNN)</b>	Classifies data based on similar classes and proximity.	Supervised
<b>Decision Tree</b>	A regression tree and classification method used for decision support.	Supervised
<b>Logistic Regression</b>	Primarily used for binary and multi-class classification problems.	Supervised
<b>XGBoost Algorithm</b>	Utilizes parallel processing and optimization techniques for efficient execution on large datasets.	Supervised
<b>LightGBM Algorithm</b>	A high-performance gradient boosting framework based on decision tree algorithms.	Supervised
<b>K-Means Clustering</b>	An unsupervised learning method for grouping similar samples into identical clusters.	Unsupervised
<b>VBGMM Clustering</b>	Specifically designed for analyzing and clustering complex and heterogeneous data.	Unsupervised
<b>Generative Adversarial Networks (GAN)</b>	A neural network that generates fake data to train discriminators. The generator learns to produce acceptable data.	Unsupervised
<b>Adaptive Neuro-Fuzzy Inference System (ANFIS)</b>	Provides fast learning capacity and adaptive interpretive capabilities for modeling complex patterns and understanding nonlinear relationships.	Supervised
<b>Random Forest</b>	Classification methods that operate by combining numerous decision trees.	Supervised
<b>Naïve Bayes Algorithm</b>	A classification algorithm that can predict group membership.	Supervised

### 3. Research Background

The history of the emergence of machine learning models can be traced back to the first mathematical model of neural networks, introduced in the scientific paper by & Warren McCulloch & Walter Pitts<sup>1</sup> titled

<sup>1</sup> McCulloch, W. S., & Pitts, W. (1943). A logical calculus of the ideas immanent in nervous activity.

"Logical Calculus of Ideas Immanent in Nervous Activity" published in 1943. The first direct application of machine learning models in fraud detection is related to a study conducted by Johan Perols<sup>2</sup> in 2011, titled "Fraud Detection in Financial Statements: An Analysis of Statistical and Machine Learning Algorithms." In this study, Prelle evaluated several algorithms, including logistic regression and support vector machines (SVM), and demonstrated the potential of machine learning in providing predictive capabilities for fraud detection, which led to more efficient identification of fraudulent activities.

With the identification of the significant potential of machine learning models in fraud detection, numerous continuous studies and evaluations have been conducted. Table 2 presents a selection of the most recent studies in this field from the past five years.

**Table 2: Some of the Latest Studies on the Application of Machine Learning in Financial Fraud Detection**

No.	Researcher(s) and Year	Study Title	Study Objective	Method Used	Findings
1	Taghva, M. R., Mansouri, T., Feizi, K., & Akhgar, B. (2016)	An Intelligent System for Fraud Detection in Coin Futures Market's Transactions of Iran Mercantile Exchange Based on Bayesian Network.	To identify and prevent fraudulent activities in the coin futures market using advanced analytical models.	Utilization of a Bayesian classification model and K-means clustering for data labeling and analysis of important dependencies among data features.	The proposed model successfully distinguishes fraudsters from legitimate traders with an accuracy of 94.55%.
2	Ashish K Saxena & Aidar Vafin (2019)	Using Machine Learning and Big Data Analytics for Fraud Detection Systems in the U.S. Fintech Industry	To examine the use of machine learning models and big data analytics to prevent financial fraud in the U.S. fintech environment	Machine learning models such as Decision Trees, SVM, Random Forest, Neural Networks, and anomaly detection algorithms	Machine learning models can identify complex fraud patterns, helping financial institutions prevent fraud. Challenges include managing high-dimensional data and adapting to evolving fraud tactics.
3	Matar Al Marri & Ahmad AlAli (2020)	Financial Fraud Detection Using Machine Learning Models	To solve fraud detection problems using supervised machine learning models and compare classification techniques	Exploratory data analysis, machine learning model creation, and performance evaluation with metrics like confusion matrix and AUC	Developed a framework for financial fraud detection with high accuracy.
4	Najmeddine Dhieb & Et Al (2020)	Secure AI-Based Architecture for Automating Insurance Systems: Fraud Detection and Risk Assessment	Developing a blockchain and AI-based smart insurance system (SISBAR) for claim automation, risk assessment, and fraud detection	Using the XGBoost algorithm and comparing its performance with other advanced algorithms	XGBoost showed 7% higher accuracy compared to Decision Trees. The integration of AI and blockchain significantly improves insurance performance.
5	KanagaSuba Raja, S. (2021)	A Novel Fraud Detection Scheme for Credit Card Usage Employing Random Forest Algorithm	improve accuracy and adapt to changing user behavior	using the Random Forest algorithm combined with a feedback mechanism	The proposed fraud detection scheme using Random Forest and a feedback mechanism significantly improves detection accuracy, adapts

<sup>2</sup> Perols, J. (2011). Financial statement fraud detection: An analysis of statistical and machine learning algorithms.

No.	Researcher(s) and Year	Study Title	Study Objective	Method Used	Findings
		Combined with Feedback Mechanism			to user behavior changes, and outperforms existing methods.
6	Lellis Moreira & Et Al (2022)	Exploratory Analysis and Implementation of Machine Learning Models for Fraud Detection in Banking Systems	Evaluating machine learning models to identify suitable techniques for fraud detection	Models like Logistic Regression, Naive Bayes, KNN, and Perceptron; used SMOTE and ADASYN for data balancing	Logistic Regression and KNN performed best on balanced datasets for fraud detection.
7	Hashemi Seyedeh & Et Al (2022)	Fraud Detection in Banking Data Using Machine Learning Techniques	Proposing optimized methods for fraud detection	Algorithms such as CatBoost, XGBoost, and LightGBM combined with deep learning for enhanced performance	LightGBM and XGBoost achieved ROC-AUC of 0.95 and F1-Score of 0.79. Bayesian optimization improved fraud detection accuracy.
8	Ravi Teja Potla (2023)	AI in Fraud Detection: Real-Time Financial Security	Investigating the use of real-time machine learning models for fraud detection transformation	Reviewing various real-time machine learning methods and their technical deployment challenges	Real-time models enable faster and more accurate fraud detection, ensuring financial security and customer trust.
9	Etemi Joshua Garba & Usman Idris Isma'il (2024)	Neuro-Fuzzy Models for Fraud Detection and Prevention in E-Banking	Developing a neuro-fuzzy model (ANFIS) for fraud detection in banking transactions	Addressing limitations of traditional methods and highlighting the need for machine learning techniques	Neuro-fuzzy models effectively improve fraud detection and prevention accuracy and efficiency.
10	Dr. V. Govindan & Et Al (2024)	Fraud Detection in Online Transactions in the Banking Sector	Enhancing fraud detection accuracy in online banking	Models like Logistic Regression, Decision Trees, Random Forest, and SVM	Random Forest demonstrated the highest accuracy, while feature engineering and ensemble methods reduced false positives and improved detection rates.
11	Najwan Thair Ali & Et Al (2024)	Enhancing Credit Card Fraud Detection Using Machine Learning and GAN	Improving fraud detection through data balancing with GAN	A hybrid model combining Decision Trees, Logistic Regression, and Naive Bayes; evaluated using precision, recall, and F1-Score	GAN achieved 99.9% accuracy and F1-Score, proving highly effective for balancing datasets and improving fraud detection accuracy.
12	Joy Phiri & Et Al (2024)	Online Banking Fraud Detection: A Comparative Study of South Africa and Spain	Examining online banking fraud detection challenges in South Africa and Spain	Design Science Research (DSR), data collected via focus groups and semi-structured interviews	Identified challenges: South Africa lacks online fraud experts and efficient systems; Spain faces inadequate regulatory frameworks.
13	Vibhuti Talreja & Et Al (2024)	A Study on AI Applications in Fraud Detection	Comparing AI tools with traditional methods for fraud detection	Reviewing literature on AI's role in fraud detection, customer experience improvement, and financial institution	AI revolutionizes financial fraud detection by identifying complex fraud patterns, enhancing prevention strategies, and improving operational efficiency.



No.	Researcher(s) and Year	Study Title	Study Objective	Method Used	Findings
14	Himanshu Sinha (2024)	Analysis of Credit Card Fraud Detection Systems Based on Machine Learning	Evaluating machine learning systems for detecting credit card fraud	performance enhancement Classification models such as XGBoost, SVM, Random Forest, Decision Tree, and Bagging	XGBoost achieved 99% accuracy; Bagging had the highest F1-Score (95%).
15	Njoku, D. O & Et Al (2024)	Machine Learning Approach for Fraud Detection Systems in Financial Institutions	Examining machine learning models for fraud detection in financial institutions	Utilized secondary data from Kaggle's "Credit Card Fraud Detection" dataset	Proposed a system with an intuitive user interface and fraud reporting capability.
16	Jáuregui Velarde & Et Al (2024)	Financial Revolution: AI and Machine Learning Applications in Banking	Reviewing major approaches, benefits, and challenges of implementing AI/ML in banking systems	Systematic literature review using the PRISMA framework	AI/ML enhances credit risk analysis and fraud prevention but raises ethical and security concerns regarding customer data handling.
17	Al-Dahasi & Et Al (2024)	Optimizing Fraud Detection in Financial Transactions Using Machine Learning and Imbalance Reduction	Enhancing predictive performance of fraud detection systems through algorithm optimization and data imbalance reduction	Data preprocessing, feature selection, sampling, and standardization methods	XGBoost and Random Forest showed superior performance, balancing false positives and negatives effectively.

#### 4. Methodology

This study is based on the Design Science Research Methodology (DSRM), which is considered a pragmatic, solution-oriented approach. DSRM goes beyond mere description and explanation, advancing towards problem-solving. The primary goal of Design Science is to shift the focus from problem-centric to solution-centric perspectives, thus transitioning from purely descriptive-explanatory approaches to prescriptive ones.

This methodology, according to the framework by Peffers [11], consists of six stages:

Problem and motivation identification: Defining the research problem and its significance.

Defining the objectives of a solution: Outlining the solution and explaining its goals and advantages.

Design and development: Designing and developing a model to meet the solution's objectives.

Demonstration: Implementing the model and showcasing its effectiveness in addressing the problem.

Evaluation: Assessing the success of the model in solving the problem.

Publication: Disseminating and detailing the proposed model.

It is noteworthy that, given the main objective of this research—designing a model to address the challenges of machine learning models in fraud detection systems—the existing challenges were identified through a review of recent studies and research in this field. By leveraging the findings of previous studies and experts' opinions regarding solutions to these challenges, a proposed model was developed and evaluated.

## 5. Findings

### Identified challenges

Researchers have highlighted various challenges through studies conducted on the use of artificial intelligence, particularly the application of machine learning models in fraud detection. This study aims to design a comprehensive model that can minimize or, as much as possible, eliminate the identified challenges and their resulting consequences.

#### Data limitation:

Saxena [4], Al Marri [12], and Potla [2] identified data volume and data limitations as one of the fundamental challenges in their research. Collecting and training data is inherently time-consuming and costly. Consequently, most researchers applying machine learning models rely on limited, selected, or artificially generated data for model evaluation. This approach often prevents the complete identification of dataset features, leading to underfitting errors. As a result, a significant gap exists between the obtained outcomes and real-world scenarios, accompanied by an increase in false negatives.

#### Need for Data Labeling:

Supervised machine learning models require preprocessed and labeled data for classification, undermining their ability to evaluate and refine real-time transactions. Al Marri [12] also identified this issue as a significant challenge in their research.

#### Dynamic nature of fraud techniques:

Most researchers have identified the dynamic nature of fraud patterns and their rapid changes as a significant challenge in fraud detection systems. Raghavan [13] even further describes fraud as a patternless process. However, other researchers such as Saxena [4], Potla [2], Garba [1], and Govindan [3] have also highlighted the dynamic nature of fraud techniques as a challenge in their studies. Fraudsters are constantly devising new patterns and methods to evade detection. That leads to a reliance on historical data, often resulting in a significant deviation and an increased rate of false negatives.

#### Bias in machine learning models:

Potla [2], in their study on the challenges and issues of machine learning in fraud detection, highlighted an ethical consideration referred to as bias. They explained that bias in machine learning models, mainly supervised models, when identifying transactions that contain or resemble trained patterns, can increase false-positive results. This concept is closely related to overfitting, a standard error in data science.

#### Costs of misclassification in machine learning models:

Misclassifications by machine learning models can result in financial and reputational damages for financial institutions or consumers from the following perspectives:

**Losses from false negatives:** Fraudulent transactions incorrectly classified as legitimate by the model can lead to financial losses and a decrease in the credibility of the fraud detection system.

**Losses from false positives:** Halting legitimate transactions due to the model's erroneous classification of them as fraudulent can cause financial losses, harm the reputation of financial institutions, and undermine consumer trust.

#### Accountability and Transparency:

Velarde [14] identifies one of the fundamental challenges of building customer trust in artificial intelligence. Potla [2] highlights in their research that while models can provide accurate predictions, a lack of transparency fosters distrust among customers. Potla emphasizes the need to clarify who will be held

accountable in the event of a prediction error. Additionally, they assert that while models assist in the detection process, humans remain responsible for critical decisions.

**Proposed solutions of the study (objectives - design - results):**

Previous research has often focused on selecting the optimal algorithm. However, the primary challenges associated with using machine learning models—regardless of the chosen technique—have been commonly identified as limiting factors across studies. Therefore, the main objective of this research, based on the selected methodology, is to propose solutions to address these issues and design a process-oriented model to mitigate them. The selection of the algorithm (supervised or unsupervised machine learning models) does not affect the implementation process of the proposed model in the study.

Moreover, Table 3 presents the frequency of recommended algorithms from previous research to facilitate the selection of these algorithms.

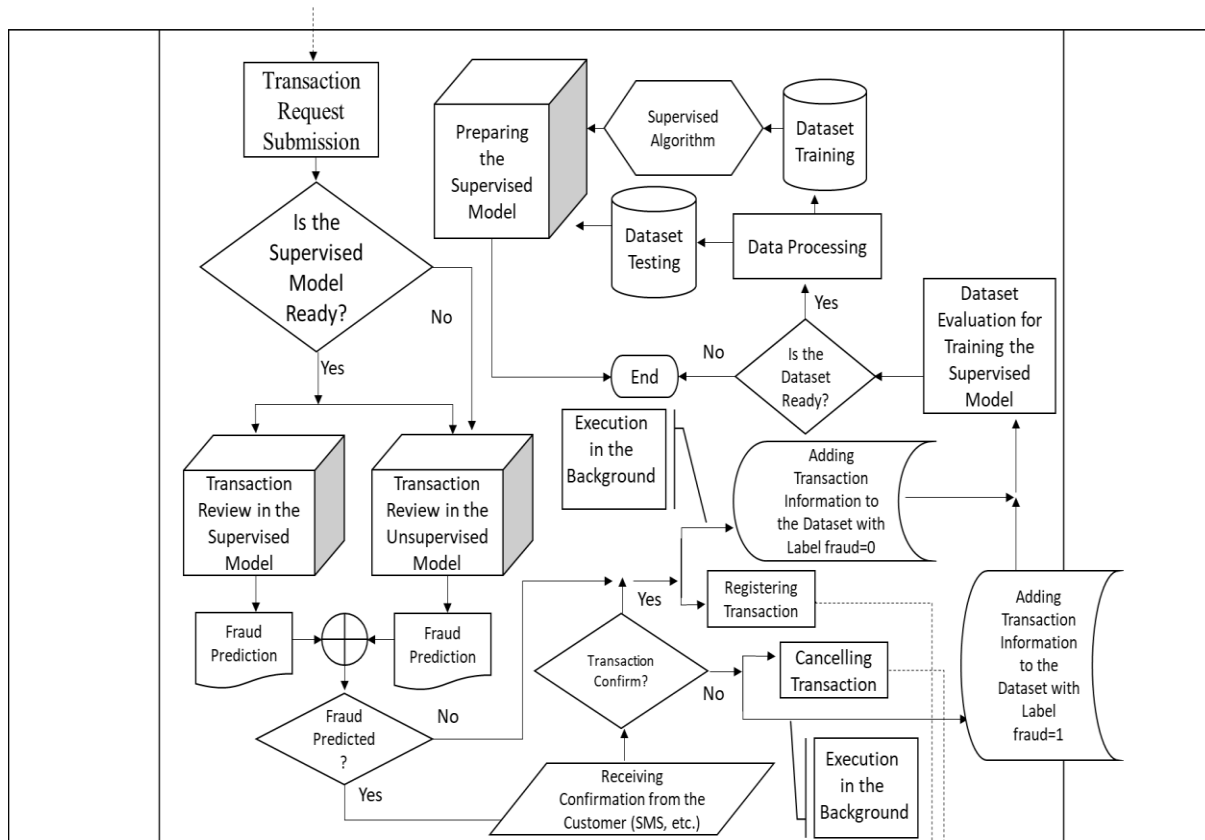
**Table 3. Distribution of Recommended Algorithms in Previous Research**

Model Name	Frequency of Recommendation
Random Forest	4
XGBoost	2
Light GBM	1
Combination of Random Forest and XGBoost	1
Combination of Light GBM and XGBoost	1
KNN & Logistic Regression	1
ANFIS	1
GAN	1
Combination of Bayesian and K-means	1

**Proposed model of the study:**

The proposed model, designed using the findings of previous studies and expert opinions on potential solutions to identified challenges, is presented as a subprocess within the primary transaction processing cycle in Figure 1. As shown, after a transaction request is logged, the fraud detection phase begins. Following the final identification of fraud patterns by the deployed models (unsupervised/supervised, with unsupervised models being deployed initially), the final decision is left to the customer. If the customer confirms the transaction as fraudulent, the identified pattern is definitively added to the training/testing dataset as a fraudulent pattern. Additionally, based on previous research, the lack of access to labeled data is a significant challenge. The proposed model starts with fraud detection using unsupervised algorithms to address this. Subsequently, after preparing datasets containing labeled information, supervised models are trained and deployed alongside the unsupervised models for subsequent transactions.





**Figure 1. Proposed Model of the Study -Transaction Registration Process**

### Model evaluation

One of the most significant operational challenges in using machine learning models for fraud detection is the limitation of data. Since the proposed model operates as a real-time subprocess within the transaction registration pathway, it does not face data collection challenges or lack of comprehensiveness in sample selection. Data flows continuously and iteratively into the system in the background, allowing for consistent updates. Once data sufficiency is evaluated, it is used to train and test the supervised model. Furthermore, as long as storage capacity permits, newly labeled data is registered and, after evaluation, utilized to retrain the model in subsequent phases.

The challenge of labeling training/testing data arises mainly when only supervised models are used for decision-making. However, this challenge is mitigated since the proposed model allows decision-making through both supervised and unsupervised methods. Additionally, when a decision is made regarding whether a transaction is fraudulent or legitimate, the new pattern is added to the dataset as labeled data (fraud = 0 or 1) for future use.

Regarding the dynamic nature of the model in learning and identifying new fraud patterns, as explained in the context of data limitations, the newly discovered patterns are stored for future training. This feature allows the proposed model to address this challenge considerably. However, it is important to acknowledge that the battle between fraud detection systems and fraudsters' evolution of new fraud techniques is ongoing. All efforts are directed toward minimizing the time gap between the emergence of new fraud patterns and their detection by fraud detection systems. Additionally, relying on historical data and training the model

based solely on it can result in bias. Continuous model updates with new data and evaluating prediction outcomes based on customer confirmation can significantly reduce model bias.

Since customer confirmation is the key factor in executing or halting the transaction registration process in the proposed model, the associated detection costs will be mitigated.

Ultimately, as the outcome of the decision-making process is entrusted to the customer, they will gain a comprehensive understanding of the process and share responsibility for the transaction execution.

## 6. Conclusion

Based on the study's findings, the challenges identified in the literature related to fraud detection in banking transactions include data limitations, labeled data, discovering new fraud patterns, bias, detection costs, and accountability. Utilizing a data science research methodology, this study aimed to address these issues and propose solutions.

The proposed model is designed to address the challenges of implementing machine learning models in fraud detection systems by continuously learning from fresh data streams. It operates online, completing the fraud detection process as a repetitive cycle, and leverages the final labeling of data in the short term to enhance the training process, thereby reducing false positive errors.

Additionally, the dual decision-making process, enabled by simultaneously deploying unsupervised and supervised algorithms, helps reduce false harmful errors to some extent. However, further efforts to minimize such errors could be explored in future research.

It is also recommended that future studies evaluate the optimal combination of supervised and unsupervised techniques to determine the synergistic accuracy of these approaches in fraud detection.

## References

1. Vasudevan S, Govindan V, Byeon H. Online transaction fraud detection in the banking sector using machine learning techniques. *Edelweiss Appl Sci Technol*. 2024;8(5):864-72.
2. Potla RT. AI in fraud detection: Leveraging real-time machine learning for financial security. *J Artif Intell Res Appl*. 2023;3(2):534-49.
3. Hashemi SK, Mirtaheri SL, Greco S. Fraud detection in banking data by machine learning techniques. *IEEE Access*. 2022;11:3034-43.
4. Saxena AK, Vafin A. Machine learning and big data analytics for fraud detection systems in the United States fintech industry. *Emerg Trends Mach Intell Big Data*. 2019;11(12):1-11.
5. Thennakoon A, Bhagyani C, Premadasa S, Mihiranga S, Kuruwitaarachchi N. Real-time credit card fraud detection using machine learning. In: 2019 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence). IEEE; 2019 Jan 10–11; Noida, India. p. 488-93.
6. Minastireanu EA, Mesnita G. An analysis of the most used machine learning algorithms for online fraud detection. *Inform Econ*. 2019;23(1).
7. Alhaddad MM. Artificial intelligence in banking industry: A review on fraud detection, credit management, and document processing. *ResBerg Rev Sci Technol*. 2018;2(3):25-46.
8. Russel S, Norvig P. Artificial intelligence—a modern approach. 3rd ed. *Knowl Eng Rev*. 2012;1:78-9.
9. Talreja MV, Kumar VS, Vignesh S. A survey of AI on financial fraud detection. *EPRA Int J Environ Econ Commer Educ Manag (ECEM)*. 2024;11(5):154-7.

- 10.** Bello OA, Olufemi K. Artificial intelligence in fraud prevention: Exploring techniques and applications challenges and opportunities. *Comput Sci IT Res J.* 2024;5(6):1505-20.
- 11.** Peffers K, Tuunanen T, Rothenberger MA, Chatterjee S. A design science research methodology for information systems research. *J Manag Inf Syst.* 2007;24(3):45-77.
- 12.** Al Marri M, AlAli A. Financial fraud detection using machine learning techniques [thesis]. Rochester, NY: Rochester Institute of Technology; 2020.
- 13.** Raghavan P, El Gayar N. Fraud detection using machine learning and deep learning. In: 2019 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE). IEEE; 2019 Dec. p. 334-9.
- 14.** Usman M, Garba EJ, Ismai'il UI. Neuro-fuzzy models for electronic banking fraud detection and prevention: A review of recent advances. *Int J Res Innov Appl Sci (IJRIAS).* 2024;7(9):406-14.