SCIENTIFIC OASIS

Journal of Intelligent Decision Making and Granular Computing

Journal homepage: www. jidmag.org
ISSN: 3042-3759

Application of Machine Learning Techniques to Fraud Detection in Financial Transactions

Elaheh Rivandi[1, *]

[1] Department of Science in Finance, University of Arizona Global Campus, Chandler, AZ, USA.

ARTICLE INFO

Article history:
Received 2 May 2026
Received in revised form 27 June 2026
Accepted 29 July 2026
Available online 30 August 2026

Keywords:
Machine Learning; Financial Fraud Detection; Online Transactions; Blockchain; Imbalanced Data; Anomaly Detection.

ABSTRACT

The rapid expansion of e-commerce and online financial transactions has made financial fraud a serious global concern. Conventional methods based on fixed rules are often unable to detect complex fraud patterns. This study examines machine learning techniques as a more adaptive approach to identifying fraudulent transactions. The methods considered include logistic regression, random forest, XGBoost, support vector machines (SVM), bidirectional long short-term memory (BiLSTM), bidirectional gated recurrent units (BiGRU), and hybrid models. Evidence from the reviewed studies indicates that these models can achieve high fraud-detection accuracy when combined with data preprocessing, effective feature selection, and methods for handling class imbalance. Integrating machine learning with technologies such as blockchain and applying optimization methods have also improved the security and reliability of financial systems. These approaches can reduce false positives while supporting real-time detection and the processing of large volumes of transaction data.

1. Introduction

In the digital era, financial transactions form the backbone of the global economy and are conducted daily at high speed and on a vast scale. Electronic banking, e-commerce, and digital payments have largely replaced traditional methods. Although this shift has made financial interactions easier, it has also created new opportunities for abuse and fraud. Financial fraud causes substantial economic losses to organizations and customers and can severely damage public trust in financial systems. International reports estimate that billions of dollars are lost each year because of fraudulent financial transactions, increasing the need for intelligent and efficient fraud-detection and prevention systems [1].

Traditional fraud-detection methods rely mainly on fixed rules or classical statistical models. Although these approaches have detected some forms of fraud in the past, they lack the flexibility needed to recognize the complex and changing patterns devised by fraudsters. Static rule-based systems cannot readily identify previously unseen fraud schemes, while statistical models often perform poorly when applied to large, imbalanced datasets. Many of these methods also require

* *Corresponding author.*
E-mail address: elaheh.rivandi.research@gmail.com

https://doi.org/10.31181/jidmgc21202647

manual configuration and cannot process transactions in real time, limiting their usefulness in modern financial environments [2].

Machine learning provides a more adaptive approach. Its algorithms can analyze large datasets, uncover hidden patterns, and adjust to changing conditions, allowing fraudulent activity to be identified dynamically and in real time. In addition to improving detection accuracy, predictive models can help organizations take preventive action before losses occur. Recent studies have reported strong results from supervised algorithms such as random forests, gradient boosting, and deep neural networks, as well as from unsupervised methods such as clustering and anomaly detection [1].

Class imbalance remains one of the main difficulties in this field because fraudulent transactions are far less common than legitimate ones. As a result, models may become biased toward classifying transactions as legitimate. Techniques such as oversampling, undersampling, and robust learning algorithms have been developed to address this problem. Feature engineering is also important because it can extract meaningful information from transaction metadata and substantially improve model accuracy.

Real-time operation imposes another requirement on financial fraud-detection systems. Models must be able to flag suspicious transactions within a fraction of a second if financial losses are to be prevented. Financial laws and regulatory requirements also oblige organizations to use explainable artificial intelligence models so that algorithmic decisions remain transparent to users and regulatory authorities [3]. User trust also affects acceptance of AI-based financial services [4].

Machine learning has changed how financial fraud-detection systems are designed and provides a basis for building more secure and trustworthy systems for digital banking and commerce [5]. Several problems nevertheless remain, including adversarial attacks against models, privacy concerns, and the scalability of processing very large datasets. Future research should therefore examine hybrid approaches, privacy-preserving techniques, and explainable models to develop resilient and sustainable systems for combating financial fraud [6]. Figure 1 presents the main stages and supporting components of machine-learning-based fraud detection in financial transactions.

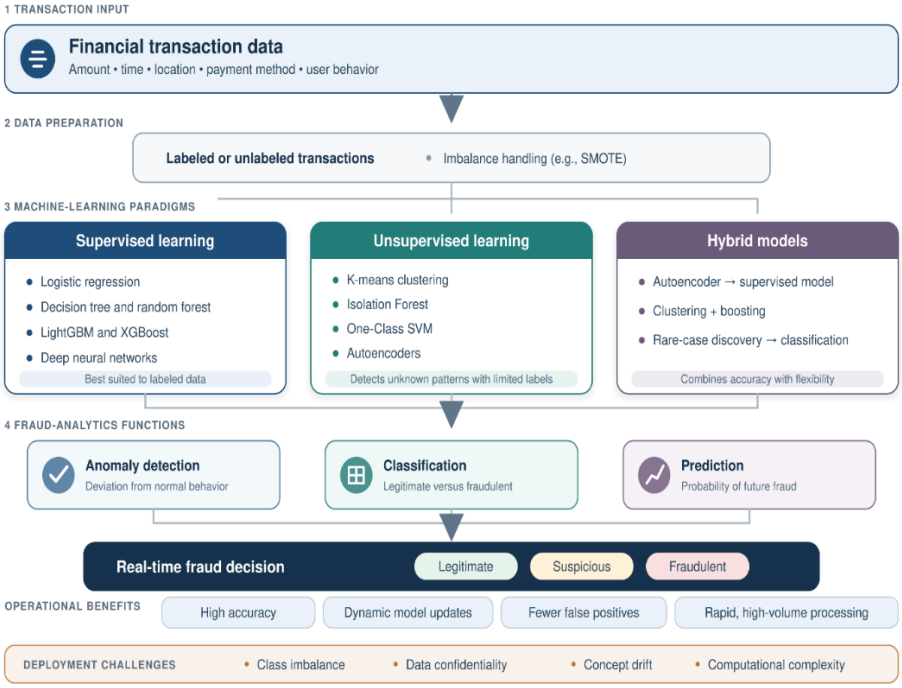

Fig. 1. Integrated machine-learning framework for fraud detection in financial transactions
Note. SVM = support vector machine; LSTM = long short-term memory; SMOTE = synthetic minority oversampling technique.

This article is organized into five sections. Following this introduction, Section 2 reviews previous studies. Section 3 provides a brief overview of machine learning techniques, while Section 4 examines selected applications of these techniques to fraud detection in financial transactions. The final section presents the general conclusions and discusses several of the main challenges that remain.

2. Literature Review

Gazi *et al,.*[7] examined the importance of fraud detection in the financial sector. As conventional methods have become less effective, alternative approaches are increasingly needed. The authors presented machine learning as a method capable of analyzing large datasets and identifying complex patterns. Their review of machine learning applications in fraud detection found that random forest performed best, achieving the highest accuracy, precision, and recall in distinguishing fraudulent from legitimate transactions.

The main strengths of the study were:

i. Methodological novelty through the use of machine learning instead of conventional methods.
ii. The capacity to process very large volumes of transaction data.
iii. The ability to identify hidden and nonlinear relationships in the data.
iv. Strong random forest performance in terms of accuracy, precision, and recall.
v. Consideration of both the potential and limitations of machine learning.

The study also had several limitations:

i. Dependence on high-quality data, as incomplete or imbalanced datasets can produce erroneous results.
ii. High computational complexity and resource requirements.
iii. The need for regular model updates because fraud patterns continually change.
iv. Limited interpretability, since many algorithms, including random forest, operate as “black-box” models whose decisions are difficult to explain.
v. Possible differences between experimental results and performance in operational environments with greater scale and complexity.

Dornadula [8] discussed the growth of credit card fraud on online platforms such as e-commerce websites. As internet-based payment methods have expanded, exposure to fraud has also increased. Their study aimed to design and develop a new method for detecting fraud in streaming transaction data. Its main objectives were:

i. Analyzing customers’ historical transactions and extracting behavioral patterns.
ii. Clustering cardholders according to their transaction volumes.
iii. Applying a sliding-window strategy to aggregate transactions and extract group-level patterns.
iv. Training several classifiers separately for the identified groups.
v. Selecting the classifier with the best performance score for fraud prediction. Pairwise-comparison ranking can also help prioritize high-performing alternatives [9].
vi. Using a feedback mechanism to address concept drift.
vii. Testing the method on European credit card fraud data.

The principal strengths of the study were:

i. Its focus on real-time and streaming data, which was more efficient than conventional approaches.
ii. Customer clustering based on transaction behavior, resulting in more accurate models.
iii. The use of a sliding window to update behavioral patterns over time.
iv. A feedback mechanism for responding to changes in fraud patterns caused by concept drift.

v. Comparison of several classification algorithms and selection of the best-performing model, thereby improving system accuracy.

The main limitations were:

i. High computational complexity due to customer clustering and the training of multiple classifiers.
ii. Dependence on data quality, since incomplete or imbalanced data can distort the results.
iii. The need to tune the sliding window carefully because window size can substantially affect performance.
iv. Scalability difficulties when processing very large volumes of real-world transactions.
v. Dependence on a particular dataset, namely the European dataset, which may limit generalizability to other regions.

Amarasinghe [10] examined the large and growing problem of financial fraud, which has developed into a multitrillion-dollar industry. They identified several serious limitations in conventional fraud-detection methods, including complex statistical models and specialist human teams:

i. Fraud is often detected after it has occurred rather than in real time.
ii. These methods are susceptible to human error.
iii. They require costly teams of specialists.
iv. They have relatively low accuracy and cannot efficiently manage very large datasets.
v. They mainly rely on discrete data, such as user accounts or IP addresses, which are no longer sufficient.

The authors therefore argued for the use of machine learning and outlier-detection methods. They examined Bayesian networks, recurrent neural networks, support vector machines, fuzzy logic, hidden Markov models, K-means clustering, and the K-nearest neighbor algorithm as possible ways to improve fraud detection in financial transactions.

The main strengths of the study were:

i. Attention to practical problems in the financial industry and the weaknesses of conventional methods.
ii. The use of machine learning and outlier detection as alternative solutions.
iii. Examination of a broad range of algorithms and comparison of their applications in fraud detection.
iv. Consideration of increasingly advanced techniques used by hackers and fraudsters.
v. Recognition of machine learning's capacity to process very large datasets and detect complex patterns.

Its limitations included:

i. *Algorithm 1*. complexity, which requires specialist knowledge and substantial computational resources.
ii. Dependence on high-quality data, as incomplete or imbalanced data reduce model accuracy.
iii. Limited interpretability, particularly for black-box models such as neural networks.
iv. The need for continual updates as fraud patterns change.
v. The possibility that experimental results will differ from those obtained in real operating environments with greater volume and complexity.

Golyeri [11] examined fraud detection in e-commerce transactions, where effective detection can prevent unauthorized activities such as identity theft and unauthorized account access. Machine learning algorithms have been widely applied to online transaction fraud because they can learn behavioral patterns and recognize discriminating characteristics, including unusual amounts, unexpected locations, and behavior outside a user's normal range. In online purchase settings,

personalized digital interactions may also shape user behavior and transaction patterns, which makes behavioral features relevant for fraud detection in e-commerce environments [12].The study applied four basic machine learning algorithms: decision tree, logistic regression, random forest, and gradient boosting (XGBoost). The data were collected from online purchases made through the Boyner Group website and mobile application. By introducing new features and comparing several classifiers, the study differed from earlier approaches.

Its principal strengths were:

i. The use of operational e-commerce data from the Boyner website and mobile application.
ii. Comparison of several basic algorithms to identify the best-performing method.
iii. Identification of discriminating behavioral features, such as unusual amounts and transaction locations.
iv. The introduction of data features that differed from those commonly used in the literature.
v. Improved fraud-detection accuracy through the combination of multiple algorithms and new features.

The study had the following limitations:

i. The data were obtained only from the Boyner Group, limiting the generalizability of the results.
ii. The analysis was restricted to basic algorithms, whereas more advanced or hybrid algorithms might perform better.
iii. Model accuracy depended on data quality and could decline when the data were incomplete or imbalanced.
iv. Scalability was not established for very large volumes of global transactions.
v. Real-time performance was not examined, making it unclear how the models would operate under live conditions.

Thennakoon [13] focused on four main types of fraud found in real transaction data. They applied several machine learning models to each fraud type and selected the best-performing method. Using appropriate performance measures, their evaluation provided a detailed guide for selecting an algorithm suited to a particular form of fraud. The study also addressed real-time fraud detection. Predictive machine learning models and an application programming interface (API) module were used to determine whether a transaction was legitimate or fraudulent. The authors also examined a new strategy for handling imbalanced data. The dataset was obtained from a financial institution under a confidentiality agreement.

The strengths of the study included:

i. A practical focus on four major types of real-world fraud.
ii. The use of several machine learning models and selection of the best method through a comprehensive evaluation.
iii. Real-time fraud detection based on predictive models and an API.
iv. A new strategy for addressing class imbalance, which is common in fraud datasets.
v. The use of operational data from a financial institution, supporting the practical relevance of the results.

The study had several shortcomings:

i. Restricting the analysis to four fraud types may have excluded other important patterns.
ii. Technical details concerning the API and model implementation were limited and may be insufficient for reproducing the results. Domain-oriented test generation can support more systematic evaluation of software-based detection components [14].
iii. The confidential nature of the data prevents other researchers from replicating the study easily.

iv. Model comparisons may have been influenced by the selected evaluation measures, limiting the generalizability of the results.

Further limitations were:

i. Data confidentiality prevents public access and independent validation.
ii. Class imbalance remains a substantial problem despite the proposed strategy.
iii. The results may be valid only for the type of data obtained from the participating financial institution and could differ in other environments.
iv. Real-time detection requires substantial computing infrastructure, which may not be available to all banks and financial institutions.

Financial fraud in the United States has become increasingly sophisticated, with fraudsters using methods that can evade conventional detection systems. The increasing popularity of digital payments has been accompanied by growth in both the number and complexity of fraud cases, causing substantial losses to institutions and consumers. Rahman [15] sought to design and implement machine learning models that could improve the accuracy of fraud-detection systems. Their study focused on the US financial system and examined artificial intelligence approaches for anomaly detection and risk analysis. The data included transaction time, amount, and sender–receiver information, allowing the analysis of time-series data and behavioral patterns. Similar machine-learning methods have been used for financial time-series prediction under changing conditions [16].

Three models were evaluated: random forest, logistic regression, and support vector machine. Their performance was measured using accuracy, precision, recall, F1, and ROC-AUC. Random forest performed best because of its ability to handle nonlinear relationships. The findings indicated that integrating machine learning substantially improved the capacity of financial institutions to process large datasets and detect fraudulent patterns quickly. Selecting relevant features related to user behavior and transaction context also increased detection rates and reduced false positives.

The strengths of the study were:

i. Its focus on the US financial system and digital payments, which represent a current operational concern.
ii. Comparison of three commonly used machine learning models across several performance measures.
iii. Evidence of the superior performance of random forest in handling nonlinear relationships and improving accuracy.
iv. Consideration of behavioral and contextual transaction features that reduced false positives.
v. The possibility of conducting time-series analysis using time-stamped data.

The study had the following shortcomings:

i. The analysis was limited to three models, namely RF, LR, and SVM, and did not examine more advanced models such as XGBoost or LSTM.
ii. Technical details about feature selection and implementation were limited.
iii. Dependence on US-specific data may reduce the generalizability of the results to other countries.
iv. Performance was not tested under operational conditions involving very high transaction volumes or simultaneous attacks.

Its other limitations included:

i. The data came from a single transaction dataset and may not represent every type of fraud.
ii. Data confidentiality prevents public access and the reproduction of the results.
iii. The models were evaluated mainly through conventional statistical measures without considering operational or economic costs.

iv. The study concentrated on accuracy and selected features without sufficient attention to response time in operational environments.

Ashfaq [17] studied fraud and anomalies in the Bitcoin network, as well as problems commonly encountered in electronic banking and online transactions. Fraud methods have become more complex as the financial sector has developed. Although blockchain has been described as one of the most secure approaches in finance, the number of fraud cases continues to increase each year [18]. The authors therefore proposed a secure fraud-detection model combining machine learning and blockchain.

XGBoost and random forest were used to classify transactions and predict new fraud patterns. The models were trained on patterns obtained from fraudulent and legitimate transactions and then used to classify new transactions. Blockchain technology was integrated with the machine learning algorithms to detect fraudulent transactions in the Bitcoin network. Model performance was measured using precision and AUC. The researchers also conducted a security analysis of the proposed smart contract to assess the system's resilience [19]. An attacker model was developed to help protect the system against attacks and vulnerabilities.

The strengths of the study were:

i. Integration of machine learning and blockchain to improve security and reliability.
ii. The use of XGBoost and random forest, both of which can perform well when classifying complex data.
iii. Evaluation through precision and AUC.
iv. Security analysis of the smart contract, which strengthened the study's practical component.
v. Development of an attacker model to identify and address vulnerabilities.

The shortcomings were:

i. The analysis was restricted to two algorithms and did not examine alternatives such as LSTM or graph neural networks.
ii. Technical details about implementing the smart contract and attacker model were limited.
iii. The data and experimental conditions were not described fully, making the results difficult to reproduce.
iv. The exclusive focus on Bitcoin may limit the application of the model to other blockchain networks.

The study was also subject to the following limitations:

i. Dependence on characteristics specific to the Bitcoin network reduces generalizability to other financial systems.
ii. Confidentiality or the lack of public access to the datasets prevents independent validation.
iii. The proposed attacker model may cover only certain attacks and may be insufficient against more complex threats.
iv. Real-world implementation requires substantial computing and security infrastructure that may not be available in every institution.

Wireless communication systems carry very large volumes of data and must remain protected against interference. Within this setting, financial fraud has become an important concern. Almazroi [20] proposed the ResNeXt-embedded GRU (RXT), an artificial intelligence model designed to process financial transaction data in real time. The model follows a systematic pipeline that begins with data input and preprocessing. SMOTE is then applied to reduce class imbalance. Features are extracted through a hybrid autoencoder and ResNet approach known as EARN. This stage identifies relevant data patterns, while feature engineering improves the model's ability to distinguish between classes.

The classification stage is based on the RXT model, which is tuned using the Jaya optimization algorithm to produce RXT-J. The model was evaluated using three real financial transaction datasets.

Compared with existing algorithms, it improved several performance measures by 10–18% while retaining high computational efficiency. The findings indicate improvements in the security and efficiency of financial transactions. In the presence of wireless communication interference, the method also supports security, data availability, reliability, and resistance to cyberattacks.

The main objectives and contributions of the study were:

i. Introducing the hybrid RXT model, which combines ResNeXt and GRU.
ii. Applying SMOTE to address class imbalance.
iii. Combining an autoencoder and ResNet within EARN to extract effective deep features.
iv. Fine-tuning the model with the Jaya algorithm.
v. Evaluating the model on three real datasets.
vi. Obtaining improvements of 10–18% over existing algorithms across several performance measures.
vii. Addressing wireless communication security and resistance to cyberattacks.

The study had several shortcomings:

i. The evaluation was restricted to three datasets and may not generalize to other financial environments.
ii. The complexity created by combining several techniques may hinder implementation in operational settings.
iii. Technical details concerning the integration of the ResNeXt and GRU blocks and the exact SMOTE configuration were limited.
iv. Comparison was limited to the reported baseline algorithms and did not examine advanced alternatives such as XGBoost or LSTM.

The main limitations were:

i. Dependence on specific and confidential data, making reproduction difficult for other researchers.
ii. The need for substantial computing infrastructure to operate the model in real time.
iii. A focus on wireless communication security that may be less applicable to other financial settings.
iv. The possibility that Jaya optimization will perform differently with very large or more diverse datasets.

The rapid development of technology has increased the use of credit cards in place of cash, but it has also created new opportunities for fraud. According to the Nilson Report, global credit card losses were expected to exceed $35 billion by 2020. Credit card providers therefore need to offer services that reduce risks to their users. Retail service choices can also affect customer responses in digital purchasing contexts [21]. Najadat [22] proposed a method for classifying transactions as legitimate or fraudulent using the IEEE-CIS Fraud Detection dataset obtained from Kaggle.

The proposed BiLSTM-MaxPooling-BiGRU-MaxPooling model combines bidirectional long short-term memory (BiLSTM) and bidirectional gated recurrent units (BiGRU). Six other machine learning algorithms were also evaluated: Naïve Bayes, voting, AdaBoost, random forest, decision tree, and logistic regression. The proposed model outperformed these algorithms and achieved a score of 91.37%.

The principal objectives and contributions were:

i. Using a hybrid BiLSTM–BiGRU model capable of learning sequential patterns.
ii. Comparing the proposed model with several classical machine learning algorithms.
iii. Achieving an accuracy of 91.37%.
iv. Using the established IEEE-CIS Fraud Detection dataset.
v. Incorporating MaxPooling to reduce model complexity and improve computational efficiency.

The study had the following shortcomings:

i. It used only the IEEE-CIS dataset, which may limit generalizability.
ii. Technical details concerning feature selection and the precise model settings were not provided.
iii. The comparisons involved classical algorithms but did not include advanced alternatives such as XGBoost or deeper neural networks.
iv. The complexity of the hybrid model may make implementation difficult in real operational environments.

Its limitations included:

i. Dependence on Kaggle data, which may differ from data encountered in operational environments.
ii. High computational requirements for large-scale training and execution.
iii. A primary focus on accuracy, with less attention to response time and computational cost.
iv. The possibility of weaker performance when sudden changes in fraud patterns produce concept drift.

Fraud methods change as financial transactions develop, creating a need for new detection approaches. Tatineni [23] examined the integration of machine learning (ML) and blockchain technology for strengthening fraud-detection mechanisms. Machine learning algorithms, including anomaly detection and pattern recognition, can improve the identification of irregularities in financial data. Blockchain provides a secure, tamper-resistant ledger that supports transparency and traceability [24]. The article examined the applications, difficulties, and potential benefits of combining ML and blockchain for fraud detection [25]. It also presented a roadmap for developing secure and resilient financial systems.

The principal strengths of the study were:

i. Combining machine learning and blockchain to improve security and efficiency.
ii. Using anomaly detection and pattern recognition to identify fraud more accurately.
iii. Using blockchain as a tamper-resistant ledger to maintain transparency and traceability.
iv. Presenting a comprehensive roadmap for creating secure and sustainable financial systems.
v. Examining cooperation between the two technologies as a forward-looking area of development.

The shortcomings were:

i. The study was mainly conceptual and theoretical, with limited technical detail or empirical testing.
ii. It did not provide a quantitative comparison with existing methods.
iii. The complexity of integrating ML and blockchain may prevent rapid implementation in operational environments.
iv. The computational and infrastructure costs of combining the technologies were not examined fully.

The limitations included:

i. Dependence on blockchain infrastructure, which is unavailable in some financial institutions.
ii. Continuing difficulties with blockchain scalability and processing speed.
iii. The need for large and balanced datasets to train machine learning models, which may not always be available.
iv. Findings that are more suitable for theoretical guidance than immediate operational application.

The rapid expansion of e-commerce has substantially increased the use of credit and debit cards for online purchases [26]. Card fraud has grown at the same time and has become an important

global problem. Fraud affects many aspects of daily life and creates growing concern among businesses and customers. Consumer responses to online financial services are shaped partly by trust, perceived risk, and self-related evaluations, which makes customer behavior relevant to the design of fraud-prevention systems [27]. Machine learning has been applied to various problems, particularly data classification. AbdulSattar *et al.,* [28] examined binary classification, in which transactions were classified as either legitimate or fraudulent.

Five machine learning algorithms, namely SGD, decision tree, random forest, J48, and IBk, were applied to two datasets called Task1 and Task2. The accuracy of all algorithms ranged from 97.78% to 98.1%, with no substantial differences among them. Because the data were imbalanced, the Kappa statistic was also examined. Random forest produced the highest Kappa value for both datasets, whereas SGD and J48 performed worst. Other measures, including MCC, were also used, and the findings indicated that random forest performed better overall than the other algorithms.

The strengths of the study were:

i. The use and comprehensive comparison of several machine learning algorithms.
ii. Very high transaction-classification accuracy of approximately 98%.
iii. Consideration of complementary measures, including Kappa and MCC.
iv. Evidence of the superior performance of random forest under class imbalance.
v. Use of Task1 and Task2 to support the reliability of the results.

The shortcomings were:

i. The study examined only five classical algorithms and did not consider advanced models such as XGBoost or deep neural networks.
ii. Accuracy values were very similar, making the relative advantage of each algorithm difficult to establish.
iii. Technical details about data preprocessing and feature selection were limited.
iv. The weaker performance of algorithms such as SGD on Task2 indicates sensitivity to the characteristics of the dataset.

The principal limitations were:

i. Class imbalance remained a central problem and was not resolved fully through the use of complementary performance measures.
ii. The findings may apply only to Task1 and Task2 and could differ in other environments.
iii. The analysis concentrated on statistical measures and gave less attention to operational factors such as response time and computational cost.
iv. Model resistance to changes in fraud patterns caused by concept drift was not examined under real-world conditions.

Table 1 provides a comparative synthesis of the application settings, methods, findings, and limitations of the reviewed studies. The reviewed articles all addressed financial fraud detection in transaction data, but they adopted different methods. Some examined classical machine learning algorithms, including random forest, logistic regression, and decision tree, and reported acceptable performance with imbalanced data. Others used more advanced models, such as BiLSTM, BiGRU, and ResNeXt-GRU, or combined machine learning with blockchain to obtain accuracy levels of approximately 91–98% while improving security and reliability. Several studies also addressed real-time detection, time-series analysis, and class imbalance through techniques such as SMOTE. Taken together, the findings indicate that combining machine learning with technologies such as blockchain and deep neural networks can substantially improve the security and efficiency of financial systems.

Table 1
Comparative synthesis of machine-learning approaches to financial fraud detection

Study	Application context and data	Methods	Main findings and contributions	Principal limitations
[7]	Financial-sector fraud detection; review of machine-learning applications	Machine-learning models, with emphasis on random forest	Random forest produced the highest accuracy, precision, and recall for fraudulent and legitimate transactions. The study considered both the potential and limitations of machine learning.	Dependence on high-quality and balanced data; computational demands; changing fraud patterns; limited interpretability; uncertain performance under operational conditions.
[8]	Streaming transactions; European credit card fraud data	Customer clustering, sliding window, multiple classifiers, and feedback mechanism	Behavioral patterns were extracted from historical transactions. The best classifier was selected for each customer group, while the feedback mechanism addressed concept drift and supported real-time detection.	High computational complexity; sensitivity to sliding-window size; data-quality dependence; scalability concerns; limited regional generalizability.
[10]	Financial transaction fraud and outlier detection	Bayesian networks, recurrent neural networks, SVM, fuzzy logic, hidden Markov models, K-means, and K-nearest neighbor	Machine learning and outlier detection were presented as alternatives to delayed, labor-intensive, and error-prone conventional methods. The study covered a broad range of algorithms.	Algorithm ic. complexity; substantial resource requirements; sensitivity to incomplete or imbalanced data; black-box behavior; need for continual updating; limited evidence from operational environments.
[11]	Online purchases made through the Boyner Group website and mobile application	Decision tree, logistic regression, random forest, and XGBoost; new behavioral and transaction features	The study compared multiple classifiers and used features such as unusual transaction amounts and unexpected locations to improve fraud detection.	Single-company dataset; focus on basic algorithms; sensitivity to data quality and imbalance; limited scalability assessment; no real-time evaluation.
[13]	Four types of real-world fraud; confidential data from a financial institution	Multiple machine-learning classifiers, an imbalance-handling strategy, predictive analytics, and an API module	The analysis provided guidance for selecting a suitable model for each fraud type. The API enabled real-time classification of transactions as legitimate or fraudulent.	Only four fraud types were considered; limited implementation details; confidential data prevented replication and independent validation; high infrastructure requirements.
[15]	US financial transactions containing time, amount, and sender–receiver information	Random forest, logistic regression, and SVM; time-series and behavioral analysis	Random forest performed best because it could model nonlinear relationships. Behavioral and contextual features improved detection rates and reduced false positives.	Only three models were tested; limited implementation and feature-selection details; US-specific and confidential data; no assessment of operational costs, response time, extreme transaction volumes, or simultaneous attacks.

Table 1
Continued

	Study	Application context and data	Methods	Main findings and contributions
[17]	Fraud and anomalies in the Bitcoin network	XGBoost, random forest, blockchain, smart-contract security analysis, and an attacker model	Machine learning and blockchain were combined to classify Bitcoin transactions and predict new fraud patterns. Performance was assessed using precision and AUC.	Bitcoin-specific design; only two classifiers; limited technical and dataset information; restricted reproducibility; uncertain coverage of complex attacks; substantial infrastructure requirements.
[20]	Three real financial transaction datasets and real-time processing over wireless communication systems	SMOTE, EARN feature extraction, ResNeXt-embedded GRU (RXT), and Jaya optimization (RXT-J)	The model improved several performance measures by 10–18% compared with existing algorithms while maintaining high computational efficiency. It also addressed data availability, reliability, and resistance to cyberattacks.	Complex architecture; high computational requirements; limited details on model integration and SMOTE settings; uncertain generalizability; possible variation in Jaya performance at larger scales.
[22]	IEEE-CIS Fraud Detection dataset obtained from Kaggle	BiLSTM-MaxPooling-BiGRU-MaxPooling; Naïve Bayes, voting, AdaBoost, random forest, decision tree, and logistic regression	The hybrid model outperformed the classical algorithms and achieved 91.37% accuracy. MaxPooling reduced model complexity and improved computational efficiency.	Use of a single dataset; limited feature-selection and tuning details; high computational demands; restricted comparison with advanced models; limited attention to response time, computational cost, and concept drift.
[23]	Conceptual analysis of financial fraud detection	Machine learning-based anomaly detection and pattern recognition integrated with blockchain	The study explained how a tamper-resistant blockchain ledger could support transparency and traceability and presented a roadmap for secure and resilient financial systems.	Primarily conceptual; limited technical and empirical evidence; no quantitative comparison; integration and infrastructure costs not fully examined; blockchain scalability and processing-speed concerns.
[28]	Binary classification using the Task1 and Task2 datasets	SGD, decision tree, random forest, J48, and IBk	Model accuracy ranged from 97.78% to 98.1%. Random forest achieved the highest Kappa values on both datasets and performed best overall according to Kappa and MCC.	Only classical algorithms were examined; accuracy differences were small; limited preprocessing and feature-selection details; dataset-specific findings; no operational evaluation of response time, cost, or concept drift.

Note: API = application programming interface; AUC = area under the curve; BiGRU = bidirectional gated recurrent unit; BiLSTM = bidirectional long short-term memory; EARN = autoencoder–ResNet feature-extraction approach; MCC = Matthews correlation coefficient; RF = random forest; SMOTE = synthetic minority oversampling technique; SVM = support vector machine.

3. Machine Learning Techniques

Financial fraud detection generally relies on three machine learning approaches: supervised learning, including logistic regression, decision trees, random forests, gradient boosting, and deep neural networks; unsupervised learning, including clustering, anomaly detection, and autoencoders; and hybrid models that combine supervised and unsupervised methods [29]. Each approach has its own advantages and limitations. The principal techniques are discussed briefly in the following subsections.

3.1. Supervised Learning

Supervised models are trained using labeled data in which each transaction is identified as either legitimate or fraudulent. The main supervised learning techniques used for fraud detection include the following:

i. Logistic regression: Logistic regression is one of the simplest and most widely used algorithms. It estimates the probability of fraud from transaction features. Its principal advantages are simplicity and interpretability, although its performance is limited when the data contain complex and nonlinear relationships [30].
ii. Decision tree: A decision tree identifies fraud patterns by dividing the data according to selected features. The resulting structure is transparent and relatively easy to interpret, but the model may be susceptible to overfitting [31].
iii. Random forest: Random forest is an ensemble of decision trees whose predictions are combined to obtain greater accuracy [32]. Recent studies have reported good performance when this method is applied to imbalanced datasets.
iv. Gradient boosting, LightGBM, and XGBoost: These boosting algorithms improve successive models by correcting errors made by earlier ones [33]. They have achieved high fraud-detection accuracy when applied to large and complex datasets [31].
v. Deep neural networks: Deep neural networks can learn complex and nonlinear relationships, making them effective in detecting sophisticated fraud patterns [34]. Spiking neural networks are another neural-network architecture examined in hardware and software simulation studies [35]. Their application, however, requires large datasets and substantial computational resources [36].

3.2. Unsupervised learning

Unsupervised learning methods are used when labeled data are limited or unavailable. The main techniques include the following:

i. Clustering: Algorithms such as K-means divide transactions into groups with similar characteristics. Transactions that fall outside the identified clusters are treated as potentially fraudulent [37].
ii. Anomaly detection: This approach assumes that fraud is a rare event. Methods such as Isolation Forest and One-Class SVM identify transactions that differ from normal transaction patterns [38].
iii. Autoencoders: Autoencoders are neural networks trained to reconstruct legitimate transaction data. Transactions with high reconstruction errors are classified as potentially fraudulent. This method has been effective when applied to complex and unstructured data [36].

3.3. Hybrid models

Hybrid models combine supervised and unsupervised learning to draw on the advantages of both approaches. Common applications include the following:

i. Combining supervised and unsupervised methods: An autoencoder may first be used to detect anomalies, after which a supervised model is trained using its output. This combination can increase detection accuracy and reduce the error rate [39].
ii. Hybrid frameworks: Combining boosting algorithms with clustering methods can produce better performance than applying either method independently [40].

iii. Application to imbalanced data: Unsupervised methods can first identify rare observations, after which supervised models are trained using the identified samples. This procedure can reduce the effect of class imbalance [41].

Supervised learning is suitable for labeled data and can achieve high accuracy, but it depends on access to complete and balanced datasets. Unsupervised learning is useful when labeled observations are scarce and can identify previously unknown patterns. Hybrid models are considered particularly suitable for operational settings because they combine the accuracy of supervised models with the flexibility of unsupervised methods [42].

4. Application of machine learning techniques to fraud detection in financial transactions

The continued expansion of e-commerce and widespread use of credit and debit cards have made financial fraud a serious global problem. Online transactions create opportunities for abuse because of their high volume, rapid processing, and variety of payment methods. AI-mediated purchasing may also affect impulsive online decisions and transaction risk [43]. Banks and financial institutions therefore require intelligent and efficient methods for detecting and preventing fraudulent activity. Machine learning can analyze complex datasets and identify hidden patterns, making it useful in the design of fraud-detection systems.

4.1. Nature of financial transaction fraud

Financial fraud can take several forms, including unauthorized credit card use, identity theft, suspicious transactions involving unusual amounts, and abnormal patterns in purchasing or money transfers. These activities share one important characteristic: fraudulent cases are concealed within a much larger volume of legitimate transactions. Conventional systems based on fixed rules are therefore often unable to identify complex and changing fraud patterns [44].

4.2. Role of machine learning in fraud detection

Machine learning algorithms perform three main functions in financial fraud detection:

i. Anomaly detection: Identifying transactions that deviate from established patterns of normal behavior [45].
ii. Classification: Determining whether a transaction is legitimate or fraudulent.
iii. Prediction: Estimating the probability of fraud in future transactions from historical data. Hybrid forecasting models also support adaptive prediction in data-driven systems [46–48].

These functions have made machine learning a principal component of contemporary antifraud systems. Commonly applied algorithms include the following [49]:

i. Logistic regression: A simple and interpretable method for the binary classification of transactions.
ii. Random forest: A tree-based ensemble method that can handle imbalanced datasets effectively.
iii. XGBoost and AdaBoost: Boosting algorithms that can detect complex patterns with high accuracy.
iv. Support vector machine (SVM): A method suited to high-dimensional data and nonlinear patterns.
v. Recurrent neural networks (RNN, LSTM, and GRU): Models capable of analyzing sequential and time-series data, particularly financial transactions with temporal dependencies [50].
vi. Ensemble models: Combinations of several algorithms intended to increase accuracy and reduce prediction errors [51].

4.3. Challenges in applying machine learning

Several issues complicate the use of machine learning in financial fraud detection [52]:

i. Imbalanced data: Fraudulent transactions are far less frequent than legitimate ones. Methods such as SMOTE are commonly used to reduce this imbalance.
ii. Data confidentiality: Limited access to real financial data makes model training and evaluation more difficult.
iii. Concept drift: Fraudsters change their methods over time, requiring fraud-detection models to be updated.
iv. Computational complexity: Some advanced algorithms require substantial computational resources [53].

4.4. Advantages of machine learning

Machine learning offers several advantages in financial fraud detection [54]:

i. High accuracy: Machine learning models can identify complex and nonlinear patterns [55].
ii. Dynamic learning: Models can be updated as new transaction data become available.
iii. Fewer false positives: More accurate classification reduces the unnecessary blocking of legitimate transactions.
iv. Real-time application: Machine learning can process large transaction volumes within short periods.

Machine learning has improved financial fraud detection, but several limitations remain. Effective model development often requires large and balanced datasets, while advanced algorithms can impose high computational costs. Decisions made by complex models, particularly neural networks, may also be difficult to interpret. Current developments are moving toward the integration of machine learning with blockchain and explainable artificial intelligence to improve transparency and security while maintaining high detection accuracy [56].

The use of machine learning has substantially changed how fraudulent financial transactions are detected. The range of available algorithms has increased the accuracy and efficiency of antifraud systems. Further progress, however, depends on addressing class imbalance and concept drift and on developing systems that are more adaptive, secure, interpretable, and reliable for financial institutions and their customers [6].

5. Conclusion

Algorithm 2. use labeled data to identify suspicious transactions with high accuracy, while unsupervised methods can detect previously unknown patterns and anomalies. Hybrid models combine the advantages of these approaches and can improve detection performance while reducing error rates. Fraud detection nevertheless remains a dynamic and complex problem. Fraudsters continually devise new ways to evade existing systems, creating a need for models that are adaptable, resistant to manipulation, and explainable. Research in this area is increasingly examining federated learning to protect privacy, graph neural networks to analyze relationships among transactions, and explainable artificial intelligence (XAI) to improve transparency and trust [57, 58]. Network-based modelling has also been used to examine complex spatial and environmental systems [59].

The findings indicate that machine learning has substantially changed financial fraud detection. Classical algorithms such as random forest continue to provide reliable performance, whereas more advanced models, including BiLSTM, BiGRU, and ResNeXt-GRU, have achieved higher accuracy and are better able to process sequential data. Integrating machine learning with blockchain has also

increased transaction security and transparency. Machine learning can therefore be considered both an operational necessity and a strategic approach to protecting global financial systems.

The main challenges identified in financial fraud detection are summarized below [60].

i. Data imbalance: Fraudulent transactions usually account for only a small proportion of the available observations. Models may consequently become biased toward legitimate transactions and fail to identify fraud. Oversampling, undersampling, and algorithms designed for imbalanced data have been proposed, but class imbalance remains a major problem.
ii. Explainability: Advanced algorithms such as deep neural networks can perform well but often operate as "black boxes." Financial regulators and customers require transparent decisions, making the development of explainable models an important requirement.
iii. Real-time detection: Financial systems require rapid responses. Delays in identifying suspicious transactions can result in substantial losses. Designing models capable of low-latency, real-time processing therefore remains difficult.
iv. Adversarial attacks: Machine learning algorithms can be vulnerable to deliberately manipulated inputs. Fraudsters may modify transaction data to prevent models from recognizing fraudulent behavior. Developing models that can resist these attacks remains an active area of research.
v. Privacy and data security: The use of sensitive financial information requires strict privacy and security protections. Cybersecurity practices are also shaped by individual, social, and organizational factors [61].
vi. Federated learning and advanced encryption may reduce these concerns, but large-scale implementation remains difficult.
vii. Scalability: Financial systems process extremely large volumes of transactions each day. Machine learning models must therefore handle large and complex datasets efficiently. Big-data infrastructure and distributed systems offer possible solutions, but their cost and complexity create further implementation difficulties.

Machine learning provides a clear basis for improving financial fraud detection, but further progress requires deeper research and continued technical development. Combining complementary methods, improving model explainability, and addressing privacy and security requirements can support the development of safer and more reliable financial systems. Multidisciplinary decision frameworks can also support system-level planning in complex contexts [62–64].

Acknowledgement
This research was not funded by any grant.

Conflicts of Interest
The authors declare no conflicts of interest.

References

[1] Compagnino, A. A., Maruccia, Y., Cavuoti, S., Riccio, G., Tutone, A., Crupi, R., & Pagliaro, A. (2025). An introduction to machine learning methods for fraud detection. *Applied Sciences*, 15(21), 11787. https://doi.org/10.3390/app152111787
[2] Mekhlouf, H. B., Moussaid, A., & Ghanimi, F. (2023). Financial fraud detection using machine learning: A review of literature. In *International Conference on Advanced Technologies for Humanity* (pp. 49–54). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-74474-7_6
[3] Khanum, A., Chaitra, K. S., Singh, B., & Gomathi, C. (2024). Fraud detection in financial transactions: A machine learning approach vs. rule-based systems. In *2024 International Conference on Intelligent and Innovative Technologies in Computing, Electrical and Electronics (IITCEE)* (pp. 1–5). IEEE. https://doi.org/10.1109/IITCEE59897.2024.10467759

[4] Pezeshgi, A., Abarghoei, M. V., Naeimi, M., & Family, Q. (2026). Trusting the machine: How consumer trust in artificial intelligence shapes future adoption intentions. *Management Science Advances*, 3(1), 227–235. https://doi.org/10.31181/msa31202640

[5] Heidari, S., Shafiesabet, A., Darvishan, S., Karimi, R., & Sodagartojgi, A. (2026). Modeling the relationship between artificial intelligence, service innovation, and financial performance: A dual SEM–ANN perspective. *International Journal of Research in Industrial Engineering*. Advance online publication. https://doi.org/10.22105/riej.2026.554497.1713

[6] Ali, A., Abd Razak, S., Othman, S. H., Eisa, T. A. E., Al-Dhaqm, A., Nasser, M., ... & Saif, A. (2022). Financial fraud detection based on machine learning: A systematic literature review. *Applied Sciences*, 12(19), 9637. https://doi.org/10.3390/app12199637

[7] Gazi, M. S. (2023). Exploring machine learning techniques for fraud detection in financial transactions. *Chinese Journal of Geotechnical Engineering*, 45(10), 25–32. https://ytgcxb.periodicales.com/index.php/CJGE/article/view/332

[8] Dornadula, V. N., & Geetha, S. (2019). Credit card fraud detection using machine learning algorithms. *Procedia Computer Science*, 165, 631–641. https://doi.org/10.1016/j.procs.2020.01.057

[9] Mahpouya, F., Burris, C. J., Paul, H., & Nikolaev, A. (2026). Maximizing the expected value of experimentation for finding top-κ rank via aggregation of pairwise comparisons. *IISE Transactions*, 1–20. https://doi.org/10.1080/24725854.2026.2645062

[10] Amarasinghe, T., Aponso, A., & Krishnarajah, N. (2018). Critical analysis of machine learning based approaches for fraud detection in financial transactions. In *Proceedings of the 2018 International Conference on Machine Learning Technologies* (pp. 12–17). https://doi.org/10.1145/3231884.3231894

[11] Golyeri, M., Celik, S., Bozyigit, F., & Kılınç, D. (2023). Fraud detection on e-commerce transactions using machine learning techniques. *Artificial Intelligence Theory and Applications*, 3(1), 45–50. https://izlik.org/JA29JK68AN

[12] Fallahi, K., & Shabestar, M. S. (2018). Evaluation of the effectiveness of using personalized advertising on Facebook. *Journal of Marketing Research*, 3(2), 1–13. https://hal.science/hal-05517976/

[13] Thennakoon, A., Bhagyani, C., Premadasa, S., Mihiranga, S., & Kuruwitaarachchi, N. (2019). Real-time credit card fraud detection using machine learning. In *2019 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence)* (pp. 488–493). IEEE. https://doi.org/10.1109/CONFLUENCE.2019.8776942

[14] Kalaee, A., Parsa, S., & Fathi, N. (2023). COSMOS: A comprehensive framework for automatically generating domain-oriented test suite. *Information and Software Technology*, 154, 107091. https://doi.org/10.1016/j.infsof.2022.107091

[15] Rahman, M. S., Bhowmik, P. K., Hossain, B., Tannier, N. R., Amjad, M. H. H., Chouksey, A., & Hossain, M. (2023). Enhancing fraud detection systems in the USA: A machine learning approach to identifying anomalous transactions. *Journal of Economics, Finance and Accounting Studies*, 5(5), 145–160. https://doi.org/10.32996/jefas.2023.5.5.15

[16] Firoozabadi, S. S., Ansari, M., & Vasheghanifarahani, F. (2024). Crude oil trend prediction during COVID-19: Machine learning with randomized search and Bayesian optimization. *European Journal of Business and Management Research*, 9(3), 6–13. https://doi.org/10.24018/ejbmr.2024.9.3.2221

[17] Ashfaq, T., Khalid, R., Yahaya, A. S., Aslam, S., Azar, A. T., Alsafari, S., & Hameed, I. A. (2022). A machine learning and blockchain based efficient fraud detection mechanism. *Sensors*, 22(19), 7162. https://doi.org/10.3390/s22197162

[18] Samatova, V., Korchiev, N., Mansouri, S., & Anyanwu, K. (2024). Towards a smart asset model for digital assets on blockchains. In *2024 IEEE/WIC International Conference on Web Intelligence and Intelligent Agent Technology (WI-IAT)* (pp. 239–248). IEEE. https://doi.org/10.1109/WI-IAT62293.2024.00039

[19] Mansouri, S., Mohammed, H., Korchiev, N., & Anyanwu, K. (2024). Taming smart contracts with blockchain transaction primitives: A possibility? In *2024 IEEE International Conference on Blockchain (Blockchain)* (pp. 575–582). IEEE. https://doi.org/10.1109/Blockchain62396.2024.00085

[20] Almazroi, A. A., & Ayub, N. (2023). Online payment fraud detection model using machine learning techniques. *IEEE Access*, 11, 137188–137203. https://doi.org/10.1109/ACCESS.2023.3339226

[21] Krishnamoorthy, A., & Sanaei, F. (2026). The retail long game: Expanded service or extended return? *Marketing Intelligence & Planning*, 1–22. https://doi.org/10.1108/MIP-08-2025-0671

[22] Najadat, H., Altiti, O., Aqouleh, A. A., & Younes, M. (2020). Credit card fraud detection based on machine and deep learning. In *2020 11th International Conference on Information and Communication Systems (ICICS)* (pp. 204–208). IEEE. https://doi.org/10.1109/ICICS49469.2020.239524

[23] Tatineni, S. (2020). Enhancing fraud detection in financial transactions using machine learning and blockchain. *International Journal of Information Technology and Management Information Systems (IJITMIS)*, 11(1), 8–15. https://iaeme.com/Home/issue/IJITMIS?Volume=11&Issue=1

[24] Mansouri, S., Samatova, V., Korchiev, N., & Anyanwu, K. (2023). DeMaTO: An ontology for modeling transactional behavior in decentralized marketplaces. In *2023 IEEE/WIC International Conference on Web Intelligence and Intelligent Agent Technology (WI-IAT)* (pp. 171–180). IEEE. https://doi.org/10.1109/WI-IAT59888.2023.00029

[25] Korchiev, N., Pateria, A., Samatova, V., Mansouri, S., & Anyanwu, K. (2024). *Taming the beast of user-programmed transactions on blockchains: A declarative transaction approach*. arXiv preprint arXiv:2411.02597. https://doi.org/10.48550/arXiv.2411.02597

[26] Rostamian, N., Taghizadeh, A., Muselu, M. N., Lashaki, R. A., & Mirzamohammadi, M. (2026). When fulfilment fees become credit-risk levers: Evidence from a large e-commerce platform. *Risk Management*, 28(3), 46. https://doi.org/10.1057/s41283-026-00232-9

[27] Safizadeh, M., Yazdanparast, A., & Felix, R. (2026). Taking pride in vegan consumption: A construal level theory account of ad message appeal and future self connectedness. *Psychology & Marketing*, 1–26. https://doi.org/10.1002/mar.70107

[28] AbdulSattar, K., & Hammad, M. (2020). Fraudulent transaction detection in FinTech using machine learning algorithms. In *2020 International Conference on Innovation and Intelligence for Informatics, Computing and Technologies (3ICT)* (pp. 1–6). IEEE. https://doi.org/10.1109/3ICT51146.2020.9312025

[29] Salunke, Y., Phalke, S., Madavi, M., Kumre, P., Bobhate, G., Madavi, M. D., & Kumre, P. D. (2025). Fraud detection: A hybrid approach with logistic regression, decision tree, and random forest. *Cureus Journal of Computer Science*, 2. https://doi.org/10.7759/s44389-024-02350-5

[30] Wang, C., Nie, C., & Liu, Y. (2025). *Evaluating supervised learning models for fraud detection: A comparative study of classical and deep architectures on imbalanced transaction data*. arXiv preprint arXiv:2505.22521. https://doi.org/10.48550/arXiv.2505.22521

[31] Bello, O. A., Folorunso, A., Ejiofor, O. E., Budale, F. Z., Adebayo, K., & Babatunde, O. A. (2023). Machine learning approaches for enhancing fraud prevention in financial transactions. *International Journal of Management Technology*, 10(1), 85–108. https://doi.org/10.37745/ijmt.2013/vol101110

[32] Chehreh, S., & Sarabadani, A. (2024). A model based on random forest algorithm and Jaya optimization to predict bank customer churn. *Engineering Management and Soft Computing*, 9(2), 132–148. https://doi.org/10.22091/jemsc.2024.9541.1174

[33] Tazehkanda, S. A., & Wanga, M. C. (2024). Leveraging XGBoost to reduce failure, withdrawal, and dropout rates in undergraduate level mathematics/statistics education. In *Modern Management based on Big Data V*. https://doi.org/10.3233/FAIA240276

[34] Karami, M. (2022). *Machine learning algorithms for radiogenomics: Application to prediction of the MGMT promoter methylation status in mpMRI scans* [Doctoral dissertation, Politecnico di Torino]. https://webthesis.biblio.polito.it/id/eprint/24496

[35] Sedighi, S., & Cantley, K. D. (2025). Spiking neural networks with STDP: Hardware and software simulation comparison. In *2025 IEEE 68th International Midwest Symposium on Circuits and Systems (MWSCAS)* (pp. 872–876). IEEE. https://doi.org/10.1109/MWSCAS53549.2025.11244591

[36] Alonge, E. O., Eyo-Udo, N. L., Ubanadu, B. C., Daraojimba, A. I., Balogun, E. D., & Ogunsola, K. O. (2021). Enhancing data security with machine learning: A study on fraud detection algorithms. *Journal of Data Security and Fraud Prevention*, 7(2), 105–118. https://doi.org/10.54660/.ijfmr.2021.2.1.19-31

[37] Chaudhry, M., Shafi, I., Mahnoor, M., Ramírez-Vargas, D. L., Bautista Thompson, E., & Ashraf, I. (2023). A systematic literature review on identifying patterns using unsupervised clustering algorithms: A data mining perspective. *Symmetry*, 15(9), 1679. https://doi.org/10.3390/sym15091679

[38] Multani, D., Radhakrishnan, G. V., Shankar, U., Upreti, K., Gupta, K., & Tiwari, A. (2025). Fraud prevention in banking: Machine learning-driven approaches for detecting payment anomalies. In *2025 International Conference in Advances in Power, Signal, and Information Technology (APSIT)* (pp. 1–6). IEEE. https://doi.org/10.1109/APSIT63993.2025.11086276

[39] Iziduh, E. F., Olasoji, O., & Adeyelu, O. O. (2023). Unsupervised anomaly detection techniques for financial fraud using real-world transaction datasets. *International Journal of Scientific Research in Science and Technology*, 10(6), 740–753. https://ijsrst.com/IJSRST2302569

[40] Adejoh, J., Owoh, N., Ashawa, M., Hosseinzadeh, S., Shahrabi, A., & Mohamed, S. (2025). An adaptive unsupervised learning approach for credit card fraud detection. *Big Data and Cognitive Computing*, 9(9), 217. https://doi.org/10.3390/bdcc9090217

[41] Kumari, S., Jaiswal, N., Kanika, Kumar, A., & Kumar, D. (2024). Comparing the performance of supervised, unsupervised and hybrid learning on medical insurance fraud detection. In *International Conference on Advanced Network Technologies and Intelligent Computing* (pp. 198–211). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-83790-6_13

[42] Sarna, N. J., Rithen, F. A., Jui, U. S., Belal, S., Amin, A., Oishee, T. K., & Islam, A. M. (2025). AI driven fraud detection models in financial networks: A review. *IEEE Access*. https://doi.org/10.1109/ACCESS.2025.3596060

[43] Pezeshgi, A., Naeimi, M., & Family, Q. (2025). *Buying on impulse in the age of AI: Mechanisms, evidence, and moral dilemmas*. https://dx.doi.org/10.2139/ssrn.5402344

[44] Abd-Ellatif, L., Abrar, M., & Ismaeel, A. A. (2025). ATAD-Net: An adaptive deep learning framework for real-time financial fraud detection. *Advances in Artificial Intelligence and Machine Learning*, 5(2), 3988–4003. https://doi.org/10.54364/AAIML.2025.52225

[45] Indukuri, M., Eskandari, M., Kollu, S. N., Lukin, S., & Matuszek, C. (2026). *Hazard or anomaly? Evaluating VLMs for understanding dangers and discrepancies*. arXiv preprint arXiv:2607.18325. https://doi.org/10.48550/arXiv.2607.18325

[46] Bushehri, M., Modabber, N. A., Zahedi, M., Jafari, M., & Rivandi, E. (2027). A hybrid time-series and ANFIS model for rail transport energy forecasting: Leveraging stationarity for improved accuracy. *Tehnički vjesnik - Technical Gazette*, 34(1), 1–8. https://doi.org/10.17559/TV-20251121003149

[47] Etemadi, S., & Khashei, M. (2025). Financial forecasting using an intelligent model based on reliability. *Journal of Data Analytics and Intelligent Decision-making*, 1(1), 33–41. https://doi.org/10.22091/jdaid.2025.14091.1006

[48] Aziz, S. Q., Ahmed, H. G., Muhammed, K. K., Jha, K., Pranto, M. R. B. H., & Ahmed, M. S. (2026). AI-driven wastewater treatment: A review of predictive models, hybrid approaches, and optimization strategies. *Advances in Civil Engineering and Environmental Science*, 3(2), 138–152. https://doi.org/10.22034/acees.2026.577006.1042

[49] Chen, Y., Zhao, C., Xu, Y., Nie, C., & Zhang, Y. (2025). Deep learning in financial fraud detection: Innovations, challenges, and applications. *Data Science and Management*. Advance online publication. https://doi.org/10.1016/j.dsm.2025.08.002

[50] Taghizadeh, A., Behzadi, A., Fakhri, N., & Naghipour, S. A. (2026). Comparing machine learning models for stock prediction: LSTM comes out on top. *Journal of Modern Technology*, 3(1), 361–366. https://doi.org/10.71426/jmt.v3.i1.pp361-366

[51] Hajizadeh, E., & Davoodian, Z. (2025). An ensemble learning framework for credit card fraud detection using machine learning and deep learning. *Journal of Data Analytics and Intelligent Decision-making*, 1(3), 31–55. https://doi.org/10.22091/jdaid.2025.14411.1016

[52] Ngulube, P. (2025). Machine learning for fraud detection in financial transactions. *i-Manager's Journal on Computer Science*, 12(4). https://doi.org/10.26634/jcom.12.4.21306

[53] Jamshidi Gahrouei, A., & Asgharian, R. (2026). AI-driven protection schemes for modern power grids: Technologies, challenges, and opportunities. *Journal of Data Analytics and Intelligent Decision-making*, 2(1), 17–30. https://doi.org/10.22091/jdaid.2026.15133.1032

[54] Davitaia, A. (2025). Artificial intelligence and machine learning in fraud detection for digital payments. *International Journal of Science and Research Archive*, 15(3), 714–719. https://doi.org/10.30574/ijsra.2025.15.3.1784

[55] Okpo, S. O. (2025). Artificial intelligence and machine learning in wastewater process design: A state-of-the-art review. *Advances in Civil Engineering and Environmental Science*, e235341. https://doi.org/10.22034/acees.2025.550097.1033

[56] Anyanwu, K., Mansouri, S., & Adei, D. (2025). Towards declarative blockchains: A SHACL-based model for robust and efficient transactions. In *2025 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)* (pp. 1–5). IEEE. https://doi.org/10.1109/ICBC64466.2025.11114583

[57] Ashtiani, M. N., & Raahemi, B. (2021). Intelligent fraud detection in financial statements using machine learning and data mining: A systematic literature review. *IEEE Access*, 10, 72504–72525. https://doi.org/10.1109/ACCESS.2021.3096799

[58] Mojtabaee, M., Iranbanfard, S. J., Najafzadeh, S., & Kolahdoozi, M. (2026). Proposing a data governance model for fraud detection in executive agencies based on federated learning in a cloud computing environment. *Journal of Engineering Management and Soft Computing*, 12(2), 109–140. https://doi.org/10.22091/jemsc.2026.14081.1309

[59] Bevilacqua, C., Hamdy, N., & Sohrabi, P. (2025). Linking land uses and ecosystem services through a bipartite spatial network: A framework for urban CO_2 mitigation. *Sustainability*, 17(22), 10113. https://doi.org/10.3390/su172210113

[60] Abdaljawad, R. Y., Obaid, T., & Abu-Naser, S. S. (2023). Fraudulent financial transactions detection using machine learning. In *2023 3rd International Conference on Emerging Smart Technologies and Applications (eSmarTA)* (pp. 1–9). IEEE. https://doi.org/10.1109/eSmarTA59349.2023.10293697

[61] Nasiri, S., Shahabi, S., Shafiesabet, A., Talebbeidokhti, M., & Behineh, E. A. (2026). Cybersecurity in action: Unraveling the effects of individual, social, and organizational determinants. *Tehnički glasnik*, 20(2), 1–10. https://doi.org/10.31803/tg-20240627004731

[62] Bevilacqua, C., Vitiello, G., Sebillo, M. M. L., Provenzano, V., Sohrabi, P., Hamdy, N., Trapani, F., & Pizzimenti, P. (2025). A multidisciplinary approach to plan ecosystem services for cities in transition. In *Proceedings of the 16th Biannual Conference of the Italian SIGCHI Chapter* (pp. 1–1). https://doi.org/10.1145/3750069.3757877

[63] Moshrefi, M., & Behnamian, J. (2022). A multi-objective approach to portfolio optimization problem using the analytic hierarchy process (AHP) and genetic algorithm. *Engineering Management and Soft Computing*, 8(1), 49–70. https://doi.org/10.22091/jemsc.2019.1294

[64] Talebian, S., Golkarieh, A., Eshraghi, S., Naseri, M., & Naseri, S. (2025). Artificial intelligence impacts on architecture and smart built environments: A comprehensive review. *Advances in Civil Engineering and Environmental Science*, 2(1), 45–56. https://doi.org/10.22034/acees.2025.488106.1013