



SCIENTIFIC OASIS

Journal of Intelligent Decision Making and Granular Computing

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

JIDMGC

Journal of
Intelligent
Decision
Making and
Granular
Computing

Scientific Oasis

1010 <https://doi.org/10.30890/jidmag.2026.01>

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 29 May 2026

Received in revised form 30 June 2026

Accepted 1 August 2026

Available online 2 September 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]. In this context, sustainability refers to the long-term reliability and governance of fraud-detection systems, which differs from the environmental-political focus of the broader sustainability literature [7]. Figure 1 presents the main stages and supporting components of machine-learning-based fraud detection in financial transactions.

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

The reviewed literature can be organized according to the learning methods used, the source and structure of the transaction data, and the operational requirements of fraud detection. Across these categories, studies generally replace delayed, rule-based, or labor-intensive procedures with models that can process large datasets and identify nonlinear or anomalous patterns. Their conclusions are not directly comparable, however, because they draw on different fraud settings, datasets, performance measures, and implementation conditions.

2.1 Classical and comparative machine-learning methods

Studies of classical supervised learning most often compare random forest with logistic regression, decision tree, support vector machine, gradient boosting, and related classifiers. Gazi [8] reported that random forest achieved the highest accuracy, precision, and recall in distinguishing

fraudulent from legitimate transactions. Its capacity to process large transaction volumes and identify hidden nonlinear relationships was a clear advantage over conventional methods, although the study also recognized data-quality requirements, computational demands, changing fraud patterns, limited interpretability, and uncertainty about performance in operational environments. Rahman *et al.*, [9] reached a similar conclusion after evaluating random forest, logistic regression, and support vector machine on US financial transaction data containing time, amount, and sender-receiver information. Using accuracy, precision, recall, F1, and ROC-AUC, the study found that random forest performed best because it could handle nonlinear relationships. Behavioral and contextual features increased detection rates and reduced false positives, while time-stamped data permitted time-series analysis; comparable machine-learning methods have also been applied to financial time-series prediction under changing conditions [10]. The comparison was nevertheless confined to three models and one US-specific dataset, and it provided limited technical detail about feature selection, operational response time, very high transaction volumes, simultaneous attacks, and economic costs.

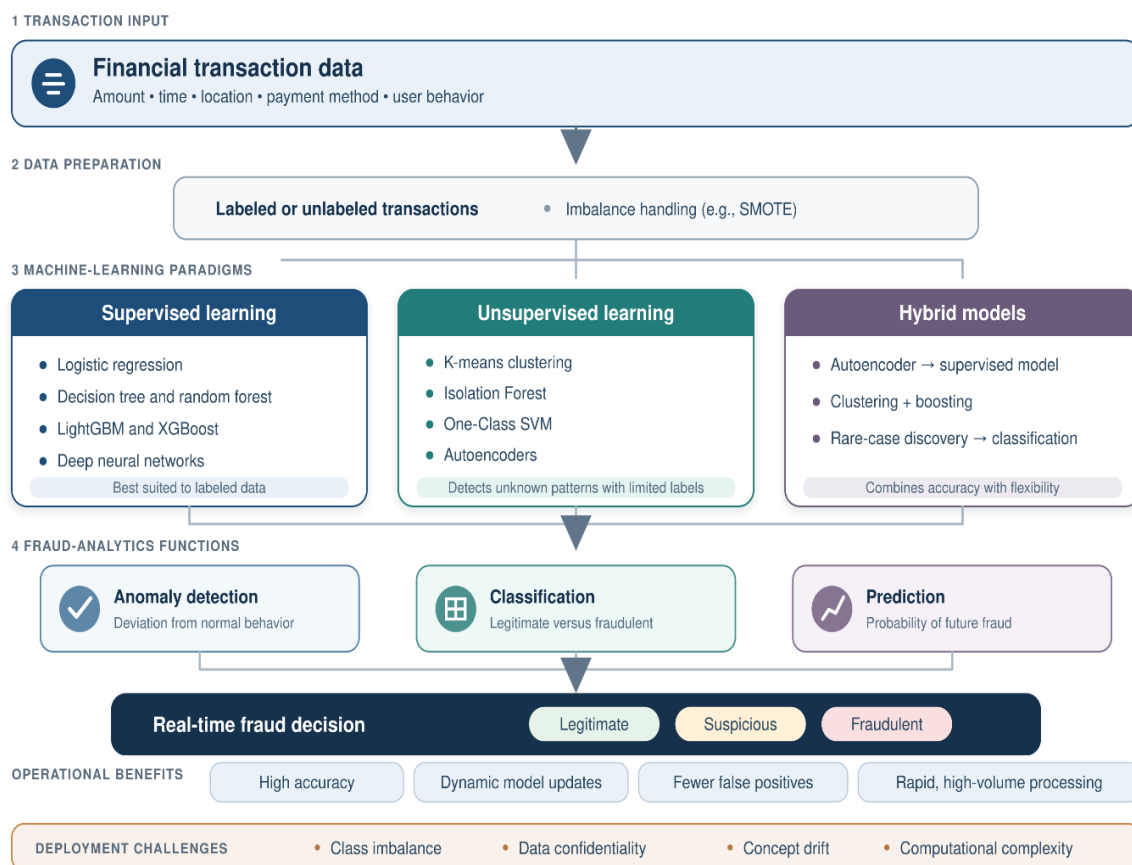


Fig. 1. Integrated machine-learning framework for fraud detection in financial transactions

Note. SVM = support vector machine; LSTM = long short-term memory; SMOTE = synthetic minority oversampling technique.

Evidence from e-commerce and FinTech transactions also favors random forest, but the results remain closely tied to the datasets examined. The rapid expansion of e-commerce has increased the use of credit and debit cards for online purchases [11], creating more exposure to card fraud. Golyeri *et al.*, [12] compared decision tree, logistic regression, random forest, and gradient boosting (XGBoost) using purchases from the Boyner Group website and mobile application. The study

introduced behavioral and transaction features, including unusual amounts, unexpected locations, and deviations from a user's normal behavior, to identify activities such as identity theft and unauthorized account access. It reported improved detection accuracy through the comparison of several classifiers and the use of new features. AI-based personalization can shape consumer spending and transaction patterns in e-commerce, making behavioral transaction data relevant to the analysis of online activity [13]. More broadly, trust, perceived risk, and self-related evaluations can affect customer responses to online financial services and are therefore relevant to the design of fraud-prevention systems [14, 15]. The single-company dataset, restriction to basic algorithms, lack of real-time evaluation, and untested scalability to global transaction volumes limit the reach of these findings. AbdulSattar and Hammad [16] compared SGD, decision tree, random forest, J48, and IBk on the Task1 and Task2 datasets. Accuracy ranged from 97.78% to 98.1%, with little separation among the algorithms. Because the data were imbalanced, the authors also examined Kappa and MCC; random forest produced the highest Kappa value on both datasets, whereas SGD and J48 performed worst. This broader evaluation supports random forest under class imbalance, but the analysis did not fully resolve the imbalance problem or test advanced models, response time, computational cost, or resistance to concept drift under operational conditions. Limited reporting of preprocessing and feature selection, together with the sensitivity of SGD on Task2, further constrains interpretation.

Broader comparisons show that model choice depends on the fraud problem and the information available. Amarasinghe *et al.*, [17] characterized financial fraud as a multitrillion-dollar problem and contrasted machine learning and outlier detection with conventional methods that often identify fraud only after it occurs, are susceptible to human error, require costly specialist teams, have relatively low accuracy on very large datasets, and depend mainly on discrete identifiers such as user accounts or IP addresses. The study considered Bayesian networks, recurrent neural networks, support vector machines, fuzzy logic, hidden Markov models, K-means clustering, and K-nearest neighbor. This breadth clarified the range of possible applications and the ability of machine learning to process large datasets and detect complex patterns, but it also exposed common requirements for specialist knowledge, substantial computing resources, high-quality data, continual updating, and evidence from realistic operating environments. Neural networks in particular raise black-box concerns that were not resolved by comparing additional algorithms.

2.2 Deep and hybrid learning methods

Deep and hybrid neural architectures produced strong results when sequential structure and learned features were incorporated. Almazroi and Ayub [18] proposed the ResNeXt-embedded GRU model (RXT) for real-time financial transaction processing in wireless communication systems. After preprocessing, SMOTE reduced class imbalance, and EARN combined an autoencoder with ResNet to extract deep features. The RXT classifier was then tuned with the Jaya optimization algorithm to form RXT-J. Across three real financial transaction datasets, the model improved several measures by 10-18% over the reported algorithms while maintaining high computational efficiency. It also addressed data availability, reliability, resistance to cyberattacks, and transaction security under wireless communication interference. These gains came from a complex pipeline, however, and the study provided limited detail about the integration of ResNeXt and GRU and the exact SMOTE configuration. Evaluation on only three datasets, limited comparison with advanced alternatives such as XGBoost or LSTM, substantial real-time infrastructure requirements, the wireless-security focus, and possible variation in Jaya's performance on larger or more diverse data leave its wider applicability uncertain.

Najadat *et al.*, [19] used the IEEE-CIS Fraud Detection dataset from Kaggle to compare six classical algorithms, namely Naive Bayes, voting, AdaBoost, random forest, decision tree, and logistic

regression, with a BiLSTM-MaxPooling-BiGRU-MaxPooling model. The hybrid architecture learned sequential patterns and used MaxPooling to reduce complexity and improve computational efficiency. It outperformed the classical models with an accuracy of 91.37%. The result supports combining bidirectional long short-term memory and bidirectional gated recurrent units, but evidence from a single Kaggle dataset may not transfer to operational data. Missing details about feature selection and model settings, the absence of comparisons with XGBoost or deeper neural networks, high computational requirements, and limited analysis of response time, computational cost, and sudden concept drift also make operational implementation difficult. The motivation for this work was the growth of credit card use and fraud; the Nilson Report expected global credit card losses to exceed \$35 billion by 2020. Retail service choices may also affect customer responses in digital purchasing settings [20].

2.3 Datasets and generalizability

The datasets used across the literature differ substantially in accessibility and representativeness. Public or named datasets, including European credit card data [21], the IEEE-CIS dataset [19], and Task1 and Task2 [16], support comparison but may not reproduce the scale, regional characteristics, and rapidly changing patterns of operational environments. Company-specific data from Golyeri *et al.*, [12] provide direct e-commerce evidence but restrict generalizability beyond one organization. Rahman *et al.*, 's US data [9] are similarly context dependent. Thennakoon *et al.*, [22] used operational data from a financial institution under a confidentiality agreement and examined four major fraud types. This improved practical relevance, but the restriction to four types may exclude other patterns, and confidentiality prevents public access, reproduction, and independent validation. The selected evaluation measures may also affect model rankings. Limited technical reporting of the API and implementation reduces reproducibility, although domain-oriented test generation could support more systematic evaluation of software-based detection components [23]. Together, these differences show why high scores from one dataset cannot be treated as evidence of equivalent performance across institutions, regions, and fraud types.

2.4 Approaches to class imbalance

Class imbalance is a shared methodological problem because fraudulent transactions are much less frequent than legitimate ones. Some studies acknowledged the issue without fully correcting it [8, 12, 17], while AbdulSattar and Hammad [16] supplemented accuracy with Kappa and MCC. Thennakoon *et al.*, [22] proposed a new imbalance-handling strategy, and Almazroi and Ayub [18] applied SMOTE before feature extraction. These approaches improve evaluation or rebalance the training data, but they do not remove dependence on data quality or establish that performance will persist across datasets. Thennakoon's strategy still left class imbalance as a substantial concern, and the exact SMOTE configuration in Almazroi and Ayub [18] 's pipeline was not reported in sufficient detail. The literature therefore differs both in how imbalance is handled and in whether performance measures reflect minority-class detection.

2.5 Real-time detection and concept drift

Real-time detection and adaptation to changing fraud patterns distinguish operational systems from retrospective classification studies. Dornadula and Geetha [21] analyzed historical customer transactions, clustered cardholders by transaction volume, applied a sliding window to aggregate transactions and extract group-level patterns, trained classifiers for the resulting groups, and selected the best-performing classifier. Pairwise-comparison ranking can also be used to prioritize high-performing alternatives [24]. A feedback mechanism addressed concept drift, and testing on

European credit card data supported a streaming application. The approach adapts behavioral patterns over time, but customer clustering and multiple classifiers increase computational complexity, window size requires careful tuning, and large-scale performance remains uncertain. Thennakoon *et al.*, [22] used predictive models and an application programming interface to classify transactions in real time, but the study gave limited implementation detail and required substantial computing infrastructure. By contrast, real-time behavior was not tested by Golyeri *et al.*, [12], and the studies by Rahman *et al.*, [9], Najadat *et al.*, [19], and AbdulSattar and Hammad [16] paid insufficient attention to operational response time or concept drift. Thus, reported predictive accuracy does not by itself establish suitability for live deployment.

2.6 Machine learning and blockchain

A separate group of studies combined machine learning with blockchain to strengthen transaction security and traceability. Ashfaq *et al.*, [25] used XGBoost and random forest to classify fraudulent and legitimate Bitcoin transactions and predict new fraud patterns. Blockchain integration was assessed through precision and AUC, a security analysis of the smart contract, and an attacker model intended to identify vulnerabilities and improve resilience. The approach responded to continuing fraud in electronic banking and online transactions despite blockchain's characterization as a secure financial technology [26], and the security analysis added an operational component [27]. Its scope was limited to two algorithms and the Bitcoin network, however, while incomplete descriptions of the data, experimental conditions, smart-contract implementation, and attacker model hinder reproduction. Public access to the datasets was also limited, and the attacker model may not cover more complex threats. Extending the model to other blockchain networks or financial systems would require substantial computing and security infrastructure.

Tatineni [28] likewise examined machine learning and blockchain, but at a conceptual level. Machine-learning methods such as anomaly detection and pattern recognition were paired with blockchain's secure, tamper-resistant ledger to support transparency and traceability [29]. The article discussed applications, difficulties, and potential benefits [30] and offered a roadmap for secure and resilient financial systems. Unlike Ashfaq *et al.*, [25], it did not provide empirical testing or quantitative comparison. Its proposals therefore remain more suitable for theoretical guidance than immediate operational use, particularly because integration complexity, infrastructure cost, blockchain availability, scalability, processing speed, and the need for large balanced training datasets were not resolved.

2.7 Interpretability, reproducibility, and research gaps

Interpretability, reproducibility, and deployment cost cut across the methodological groups. Random forest and neural models can capture complex relationships, but their black-box behavior limits explanation [8, 17]. Deep and hybrid pipelines add further difficulty because their many processing, feature-extraction, optimization, and classification stages require specialist knowledge and extensive computational resources [18, 19]. Confidential or incompletely described datasets and implementations prevent independent validation in several studies [9, 18, 22, 25]. These recurring limitations should be interpreted collectively: improvements in accuracy, precision, recall, AUC, Kappa, or MCC do not demonstrate that a model is explainable, affordable, scalable, reproducible, or stable when fraud patterns change.

Table 1 provides a comparative synthesis of the application settings, methods, findings, and limitations of the reviewed studies.

Table 1

Comparative synthesis of machine-learning approaches to financial fraud detection

Study	Application context and data	Methods	Main findings and contributions	Principal limitations
[8]	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.
[21]	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.
[17]	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.	Algorithmic complexity; substantial resource requirements; sensitivity to incomplete or imbalanced data; black-box behavior; need for continual updating; limited evidence from operational environments.
[12]	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.
[22]	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.
[9]	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	Principal limitations
[25]	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.
[18]	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.
[19]	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.
[28]	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.
[16]	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.

The comparison reveals several connected research gaps. Classical models, particularly random forest, often perform well, but most comparisons use a limited set of algorithms and context-specific datasets [8, 9, 12, 16]. Deep and hybrid models report higher or competitive predictive performance, yet their computational requirements, incomplete implementation details, and dependence on

single or small collections of datasets restrict reproducibility and generalizability [18, 19]. Approaches to class imbalance range from supplementary measures to SMOTE and newly proposed strategies, but their effectiveness has not been established consistently across institutions and fraud types [22], [16, 18]. Real-time studies address streaming data, APIs, sliding windows, and concept drift, although few evaluate response time, scalability, and adaptation together under live transaction volumes [21, 22]. Blockchain-based studies add security and traceability, but empirical validation beyond Bitcoin and the cost of operational integration remain limited [25, 28]. Interpretability receives little direct treatment despite the use of black-box models, and confidential data or incomplete reporting frequently prevents independent validation. Research that evaluates predictive performance, minority-class detection, response time, computational cost, explainability, and cross-context generalizability within the same design is therefore still limited.

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 [31]. 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 [32].
- 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 [33].
- iii. Random forest: Random Forest is an ensemble of decision trees whose predictions are combined to obtain greater accuracy [34]. 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 [35]. They have achieved high fraud-detection accuracy when applied to large and complex datasets [33].
- v. Deep neural networks: Deep neural networks can learn complex and nonlinear relationships, making them effective in detecting sophisticated fraud patterns [36]. Spiking neural networks are another neural-network architecture examined in hardware and software simulation studies [37]. Their application, however, requires large datasets and substantial computational resources [38].

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 [39].
- 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 [40].
- 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 [38].

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 [41].
- ii. Hybrid frameworks: Combining boosting algorithms with clustering methods can produce better performance than applying either method independently [42].
- 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 [43].

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 [44].

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 [45]. 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. User-generated app reviews can also be prioritized to support developer responses on mobile platforms [46].

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 [47].

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 [48].
- 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 [49–51].

These functions have made machine learning a principal component of contemporary antifraud systems. Commonly applied algorithms include the following [52]:

- 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 [53].
- vi. Ensemble models: Combinations of several algorithms intended to increase accuracy and reduce prediction errors [54].

4.3. Challenges in applying machine learning

Several issues complicate the use of machine learning in financial fraud detection [55]:

- 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 [56].

4.4. Advantages of machine learning

Machine learning offers several advantages in financial fraud detection [57]:

- i. High accuracy: Machine learning models can identify complex and nonlinear patterns [58].
- 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 [59]. Security frameworks for SDN-enabled 5G core networks also use secure network-slicing enforcement to protect communication infrastructures [60].

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

This review examined supervised, unsupervised, and hybrid machine learning approaches to fraud detection in financial transactions. Supervised algorithms use labeled data to classify suspicious transactions, whereas unsupervised methods identify previously unknown patterns and anomalies. Hybrid models combine these capabilities and can improve detection performance while reducing error rates. Across the reviewed studies, classical algorithms, particularly random forest, provided reliable results on several transaction datasets. Deep and hybrid architectures, including BiLSTM, BiGRU, and ResNeXt-GRU, were better suited to sequential data and reported strong predictive performance, although comparisons differed in their datasets and evaluation conditions. Studies that integrated machine learning with blockchain also addressed transaction security and transparency. These findings show that model performance depends on the fraud context, the characteristics of the available data, and the operational requirements of the detection system.

The reviewed approaches offer several practical advantages: they can identify nonlinear transaction patterns, process large data volumes, detect anomalies, and support rapid classification. Their limitations are closely connected. Fraudulent observations form only a small proportion of most datasets, which can bias models toward legitimate transactions even when oversampling, undersampling, or algorithms designed for imbalanced data are used [61]. Deep neural networks and other complex models may perform well but often provide limited explanations for their decisions. This is problematic when regulators, institutions, and customers require transparent outcomes. Low-latency detection is also difficult because financial systems process large transaction volumes and delays can result in substantial losses. Models may be affected by concept drift as fraud strategies change, and deliberately manipulated inputs can prevent them from recognizing fraudulent behavior. The use of sensitive financial data introduces further privacy and security requirements; cybersecurity practices are also associated with individual, social, and organizational factors [62]. Federated learning, encryption, big-data infrastructure, and distributed systems may address parts of these problems, but their computational cost, implementation complexity, and scalability remain constraints. Big-data infrastructures also create workload-management problems, including straggler tasks that can be recognized using artificial neural networks [63].

Future research should evaluate explainable artificial intelligence and federated learning within fraud-detection settings that protect sensitive data while allowing model decisions to be examined [64, 65]. Adaptive models should be tested on real-world dynamic datasets to determine how well they respond to concept drift, new fraud patterns, and changes in class distributions. Adversarial robustness also requires direct evaluation through deliberately manipulated transactions rather than reliance on conventional predictive measures alone. Graph neural networks may support the analysis of relationships among transactions, but their value should be established using financial fraud data; network-based modelling in other complex domains does not by itself demonstrate effectiveness in this setting [66]. Future evaluations should report minority-class detection, response time, computational cost, explainability, scalability, and performance under changing operational conditions within the same design. Multidisciplinary decision frameworks may support system-level planning [67–69], but their contribution should likewise be assessed directly in fraud-detection applications.

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., & Sodagartoigi, 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] Safizadeh, M. (2024). Towards a sustainable planet: Review of 'Global Environmental Politics' by Kütting and Herman (2018). *Markets, Globalization & Development Review*, 8(4). <https://doi.org/10.23860/MGDR-2023-08-04-04>
- [8] Gazi, M. S. (2023). Exploring machine learning techniques for fraud detection in financial transactions. *Chinese Journal of Geotechnical Engineering*, 45(10), 25–32. <https://ytcxb.periodicales.com/index.php/CJGE/article/view/332>
- [9] 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>
- [10] 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>
- [11] 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>
- [12] 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>
- [13] Turki, H. (2025). AI-powered personalization in e-commerce: Governance, consumer behavior, and exploratory insights from big data analytics. *Technology in Society*, 83, 103033. <https://doi.org/10.1016/j.techsoc.2025.103033>
- [14] 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>
- [15] Keshavarz, A., & Liu, S. (2026). Beyond satisfaction: Commitment and perceived customer lifetime value in Iranian banking. *Journal of Business and Management Studies*, 8(9), 47–58. <https://doi.org/10.32996/jbms.2026.8.9.6>
- [16] 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>

- [17] 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>
- [18] 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>
- [19] Najadat, H., Altit, 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>
- [20] 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>
- [21] 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>
- [22] Thennakoon, A., Bhagyan, 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>
- [23] 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>
- [24] Mahpouya, F., Burris, C. J., Paul, H., & Nikolaev, A. (2026). Maximizing the expected value of experimentation for finding top-k rank via aggregation of pairwise comparisons. *IIE Transactions*, 1–20. <https://doi.org/10.1080/24725854.2026.2645062>
- [25] 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>
- [26] 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>
- [27] 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>
- [28] 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.
- [29] 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>
- [30] 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>
- [31] 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>
- [32] 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>
- [33] Abbas, R., Samuel, A., Muhwati, K. B., Mavire, S., Katenda, E., & Adesokan, A. (2025). Machine learning and blockchain approaches for enhancing fraud prevention in financial transactions. *Engineering Science & Technology Journal*, 6(6), 296–312.
- [34] 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>
- [35] Tazehkanda, S. A., & Wang, 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>
- [36] 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>

- [37] 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>
- [38] 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>
- [39] 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>
- [40] 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>
- [41] Iziduh, E. F., Olosoji, 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://ijrst.com/IJRST2302569>
- [42] 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>
- [43] 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
- [44] 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>
- [45] Pezeshgi, A., Naeimi, M., & Family, Q. (2025). *Buying on impulse in the age of AI: Mechanisms, evidence, and moral dilemmas*. <https://doi.org/10.2139/ssrn.5402344>
- [46] Jafari, M., Majidi, F., & Heydarnoori, A. (2025). Prioritizing app reviews for developer responses on Google Play. arXiv preprint arXiv:2502.01520. <https://doi.org/10.18293/DMSVIVA2024-153>
- [47] 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>
- [48] 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>
- [49] 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.
- [50] 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>
- [51] 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>
- [52] 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>
- [53] 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>
- [54] 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>
- [55] 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>
- [56] 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>

- [57] 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/ijrsra.2025.15.3.1784>
- [58] 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>
- [59] 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>
- [60] Kumar, D., Hamidi, P., Rana, S. K., Rana, A. K., & Ansarullah, S. I. (2026). A unified security framework for SDN-enabled 5G core networks with secure network slicing enforcement. In *2026 IEEE 15th International Conference on Communication Systems and Network Technologies (CSNT)* (pp. 7–12). IEEE. <https://doi.org/10.1109/CSNT69054.2026.11502394>
- [61] 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>
- [62] 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>
- [63] Farhang, M., & Safi-Esfahani, F. (2020). Recognizing MapReduce straggler tasks in big data infrastructures using artificial neural networks. *Journal of Grid Computing*, 18(4), 879–901. <https://doi.org/10.1007/s10723-020-09514-2>
- [64] 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>
- [65] Mojtabae, M., Iranbanfard, S. J., Najafzadeh, S., & Kolaheidozi, 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>
- [66] Bevilacqua, C., Hamdy, N., & Sohrabi, P. (2025). Linking land uses and ecosystem services through a bipartite spatial network: A framework for urban CO₂ mitigation. *Sustainability*, 17(22), 10113. <https://doi.org/10.3390/su172210113>
- [67] 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>
- [68] Rezaee, K. (2026). Dual-branch hybrid-feature learning for imbalance-aware paediatric colonoscopy decision support with interpretable multi-scale networks. *Journal of Engineering Management and Soft Computing*, 12(2), 204–224. <https://doi.org/10.22091/jemsc.2026.14688.1327>
- [69] 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>