

Machine Learning for Financial Fraud Detection: A Survey of Algorithms and Applications

Dr. Pradeep Laxkar

Associate Professor

Department of Computer Science and Engineering ITM(SLS) University

Vadodara, Gujarat,

pradeep.laxkar@gmail.com

Corresponding Author * Dr. Pradeep Laxkar (pradeep.laxkar@gmail.com)

Received: 15 August 2026 | Revised: 18 August 2026 | Accepted: 25 August 2026

Abstract—Financial fraud has emerged as a serious challenge faced by financial institutions as a result of the rise of online banking, electronic payment systems, and electronic transactions. One of the main problems faced by advanced fraud detection solutions is that they fall behind in dealing with evolving and complicated methods of fraud. Modern fraud detection techniques make use of machine learning (ML) which allows for processing large volumes of financial data and detecting anomalies in the data, as well as suspicious trends and possible fraud. This research paper discusses the methods of financial fraud detection by means of ML in detail. It features several forms of financial frauds including credit card fraud, insurance fraud, fraud in financial statements, and cyber fraud. The research paper reviews different algorithms including Logistic Regression, Random Forest, Support Vector Machine, K-Means, Isolation Forest, and Long Short-Term Memory. It provides detailed information about supervised and unsupervised learning approaches. In addition to that, the paper discusses challenges faced by the automation of fraud detection, including unbalanced datasets, changing trends of fraud, lack of labeled data, false positives, difficulty of understanding the models, and computing power.

Keywords—Financial Fraud, Machine Learning, Fraud Detection, Deep Learning, Anomaly Detection, Credit Card Fraud.

I. INTRODUCTION

The management of deposits, payments, credit, and other financial services is very important to the development of the economy. Within this sector, effective fraud detection systems are very important for protecting transactions, reducing losses, maintaining the trust of clients, and ensuring compliance with relevant laws. The rapid development of digital financial transactions is the cause of serious problems for financial institutions as fraud is very difficult to control [1]. Fraud is quite a sophisticated form of crime that threatens the efficiency of compliance systems and harms financial integrity. Thus, it is necessary to deploy intelligent systems which are able to react to aggressive fraud patterns in order to prevent fraud. It should be mentioned that supervised learning has been a major tool in fraud detection however these types

of data often cannot be reliable of fraud detection as they do not take into account changes in fraud schemes [2].

The global economy, business honesty, and customer confidence are all under grave danger from the growing problem of financial fraud. While new digital technologies have many positive applications, they have also increased the attack surface for fraud, which has led to more complicated and difficult-to-detect scams. Manual auditing and rule-based systems are outdated detection methods that can't keep up with the complexity and volume of modern financial data in real-time, which causes huge economic losses and undermines confidence [3]. An efficient and accurate fraud detection system able to spot suspicious financial transactions. Ensuring that the payments system remains accessible to genuine users is of the utmost importance, alongside the need to prevent criminals from engaging in fraudulent transactions. Customers may have a negative experience and decide to go elsewhere if there are a lot of false positives. The existence of extremely skewed data sets is a significant obstacle to the application of ML to fraud detection. Only a small percentage of transactions in most databases are fraudulent; the rest are almost certainly real [4].

In high-stakes financial scenarios wherein ML-based systems are deployed, data drift, adversarial attacks, and operational risks can occur [5]. A considerable solution for the final detection of fraud could be rule-based hybrid AI-ML models, which seek to eliminate the contradictory limitations of both the ML approach and the usage of rules. In these hybrid systems, learning algorithms driven by data are combined with specific characteristics of rule-based approaches to increase the accuracy of detection while maintaining transparency and interpretability. By using hybrid AI-ML models in reality, companies can achieve an equilibrium between performance, compliance, and reliability of their fraud detection mechanisms [6].

Data shows that ML technology has been found to be significantly better than the traditional human-based ways of detecting fraudulent transactions. There is a necessity for the regulatory bodies and companies to use ML in order to enhance the effectiveness of fraud detection. In the case of

financial transactions, the program is able to identify suspicious transactions based on the atypical transactional patterns. One of the uses of the technology includes monitoring online banking transactions, as well as credit card fraud prevention. There are three types of ML: supervised, unsupervised and reinforcement learning. Supervised learning and reinforcement learning are regarded to be the most widely used compared with unsupervised learning because the main thing that distinguishes unsupervised learning from the other two types is the fact that unsupervised learning practices the usage of non-labelled data to find outliers and underlying tendencies [7].

A. Structure of the Paper

The structure of the paper is as follows: Financial Fraud Detection is discussed in Section II. Financial Fraud Detection Via Machine Learning is talked about in Section III. In Section IV, literature assessment of prior studies is presented, while Section V both brings the study to conclusion and provides suggestions for future work.

II. FINANCIAL FRAUD DETECTION

Financial fraud is a crime in which a person or entity deceives someone else to gain money illegally from them, as well as inflict financial damages upon them. It includes a wide variety of crimes such as falsifying financial statements, fraud in payments, stealing someone else's ID, loan frauds, and committing insurance frauds among others [8].

A. Types of Financial Fraud

The category of dishonest activities includes credit card fraud, identity theft, loan fraud, payment fraud, online banking fraud, among many others [9]. Financial fraud refers to acts that take advantage of flaws in the financial transaction or system in order to gain illegal recognition in the financial aspect or obtain relevant data. Examples of financial fraud are credit card fraud, indirect fraud, financial report deception, and illegal financial activities conducted via cyberspace [10]. The different categories are shown in Fig. 1. indicating that the specific methods of gaining illegal financial benefits are uncommon to them due to the complexity of financial fraud.



Fig. 1. Types of Financial Fraud

- **Credit Card Fraud:** Electronic financial transactions that take place without cash are known as credits in some cases [11]. Credit cards, which are tiny pieces of plastic imprinted with customer information and credit services, are widely utilized for online purchases.
- **Financial Statement Fraud:** Claiming abnormally high profits, evading taxes, artificially inflating stock values, or getting a bank loan are all examples of financial statement fraud. Organizational financial records include items such as expenditures, revenues, loans, etc., and are considered confidential data.

- **Insurance Fraud:** Insurance fraud is defined as "the practice of procuring benefits from an insurance company by means of an insurance policy" [12]. The reason why most people and businesses need insurance is because financial risks can impact any kind of transaction.
- **Financial Cyber-Fraud:** A relatively new term, "financial cyber fraud" describes any type of cybercrime committed with the express purpose of misleading financial institutions [13].

B. Sources and Causes of Financial Fraud

Financial fraud can originate from internal employees, external criminals, customers, or organized fraud networks exploiting weaknesses in financial systems. Common causes include identity theft, social engineering, insider misuse and vulnerabilities in digital payment systems [14].

- **Insider Threats:** The term "insider threat" refers to malicious behavior by employees, contractors, or partners of a bank that has access to sensitive data and internal systems [15]. It is possible for insiders to commit theft, earn money, or assist external hackers in gaining access to a system by abusing their authorized access.
- **Social engineering:** A type of assault known as social engineering can evade any and all security measures put in place. The use of either software or hardware to conduct social engineering makes prevention more difficult [16]. This is due to the fact that individuals who utilize both software and hardware are vulnerable to social engineering assaults.
- **Identity Theft:** Identity theft has many definitions, but in simple terms, it involves extracting, storing and weaponizing personal identifiable information (PII), Aadhaar number, PAN card number/JSON file holder's data, bank account number, bank passbook details biometric information such as fingerprint templates or print image to create fake accounts with dealings to drain all financial assets or to impersonate [17].

C. Deep Learning Algorithms for Fraud Detection

Financial datasets may be quite vast and multi-dimensional, yet DL algorithms can discover complicated patterns using multi-layer neural networks. Analyzing consumer behavior, transaction sequences, and other hidden links that standard approaches may ignore allows them to accurately detect complex fraud.

- **Long Short-Term Memory (LSTM):** The ability to learn long-term data dependencies is achieved by LSTM recurrent neural networks through the use of internal processes called gates, which govern the flow of input. The memory gates of LSTM models may learn which data in a sequence is critical to maintain or forget, allowing the models to store knowledge for lengthy durations.
- **Convolutional Neural Networks (CNNs):** CNNs are useful for handling structured information and detecting fraud. The idea is to deploy convolutional filters similar to how a spatial grid is used on an image. Their ability to automatically learn features hierarchically is key to being able to successfully identify complex patterns of fraud. Early levels of the model capture basic patterns, while later levels

synthesize various patterns in order to detect complex combinations.

- **Generative Adversarial Networks (GANs):** GANs utilize generator and discriminator networks that are in competition with each other. The ability of GANs to generate synthetic falsification data that can be used to train classifiers makes them an attractive potential tool for detection of fraud, particularly with imbalanced datasets [18]. The main challenges of GANs are training instability and mode collapse, where the generator produces a limited set of outputs. Although this holds great promise for the application of data augmentation, it remains problematic.

D. Emerging Technologies and Their Potential Impact on Financial Fraud Prevention

New technologies, such as AI, ML, Blockchain, and IoT, provide exciting methods for improving the prevention of financial fraud. These techniques can:

- **Analyze Large Data Sets:** Able to rapidly sort through large amounts of data to find anomalies that indicate possible fraud.
- **Predict Fraudulent Behavior:** Making use of predictive analytics based on past information and current transactions might allow for better prediction of fraudulent conduct.
- **Enhance Security:** Use blockchain technology to create transparent and secure transaction records, making them more resistant to fraud and data breaches [19].
- **Improve Customer Verification:** Utilize AI and ML for more accurate and efficient customer verification processes, reducing false positives and negatives.

E. Financial Fraud Detection Datasets

The proposed transformer architecture's performance, capacity to transfer knowledge, and general effectiveness

TABLE I. FINANCIAL FRAUD DETECTION DATASETS

Dataset	Data Type	Key Characteristics	Fraud Detection Relevance	Main Challenge
IEEE-CIS Fraud Detection Dataset	Payment transactions	Contains anonymized transaction, device, and browser information	Suitable for evaluating fraud detection sensitivity	Highly imbalanced fraud cases
European Credit Card Fraud Dataset	Credit card transactions	Contains anonymized numerical features, time, and transaction amounts	Widely used as a benchmark for fraud detection studies	Severe class imbalance
PaySim Mobile Money Simulation	Mobile money transactions	Simulates cash-in, cash-out, transfers, and payment activities	Supports analysis of behavioral fraud in mobile financial ecosystems	Simulated rather than directly observed transactions

F. Blockchain Financial Fraud Prevention

The current methods for detecting fraud in financial management may be drastically altered with the use of blockchain technology [21]. Organizations may enhance their fraud detection and prevention capabilities in many scenarios by utilizing blockchain's transparency and security. The banking and financial industry is one potential use case for blockchain technology in the fight against fraud.

III. MACHINE LEARNING-BASED FINANCIAL FRAUD DETECTION

The advent of ML has allowed for more adaptable and dynamic approaches to fraud detection [22]. In comparison to more traditional methods, ML-based algorithms have the potential to learn and adapt to new data, resulting in improved accuracy and efficiency over time. Mathematical and

were validated against three widely available datasets. The datasets in question present diverse record types of the entire pool of monetary transactions including operations of companies, transactions through credit cards, and monetary transfer systems. Table I lists common datasets used in detecting financial fraud along with their respective types of data, features of importance in fraud detection and obstacles such as class imbalance and data imitation issues.

- **IEEE-CIS Fraud Detection Dataset:** There are few publicly available datasets that compare to the IEEE-CIS dataset when it comes to detecting transactional fraud. It includes de-identified characteristics that stand in for different types of financial transactions and the corresponding browser and device details. Due to its extreme imbalance and limited number of fraud incidents, this dataset is ideal for sensitivity testing in detection.
- **Model Training on Labeled Threat Data:** Supervised learning models learn from historical data by
- **European Credit Card Fraud Dataset:** This information includes purchases made by cardholders across Europe during the month of September 2013. It is commonly utilized as a standard in research on detecting fraud [20]. The characteristics that are not times and quantities are all numerical and have been anonymized by PCA. Also, it's really skewed, which is indicative of actual fraud situations.
- **Pay Sim Mobile Money Simulation:** Pay Sim is a data-driven simulator developed by financial institutions that simulates a mobile money transfer environment. Every step of the payment process, including receiving and sending funds, is imitated. By comparing Pay Sim to the other two datasets, and gain a better understanding of behavioral fraud in mobile-based ecosystems.

statistical methods, as well as those in the fields of artificial intelligence, psychology, neurology, and information technology, are extensively used by ML techniques [23][24]. The techniques used to train models define the three primary subfields of ML: supervised, unsupervised, and reinforcement learning. The methods aid activities like pattern detection, transaction typing, anomaly identification, and prediction of possible frauds in financial systems.

A. Supervised Machine Learning Algorithms for Fraud Detection

Around 57% of the techniques identified in the literature comprise supervised learning, which is the most widely utilized technique in the study of fraud detection [25]. This type of approach allows the algorithm to identify the distinguishing characteristics of transactions by developing the models on well-labeled datasets, meaning every

transaction is already known to be either legitimate or fraudulent.

- **Random Forest (RF):** The ensemble methods combine various decision trees to enhance classification precision while successfully minimizing the overfitting inclination [26]. In the case of credit card scams and financial statement fraud detection, the performance of RF models has been stable, with them achieving 95% accuracy.
- **Extra Trees:** Extra Trees is a method similar to Random Forest, only that it is more computationally efficient. Use cases involving noisy data or a high feature count are ideal for this approach [27]. Even while Extra Trees uses an ensemble of decision trees, the selection of splits is more randomly distributed, making it more comparable to RF.
- **Logistic Regression (LR):** Highly regarded for its clarity and ease of understanding. Based on the features of a transaction, it predicts the likelihood of fraud. Although LR could have trouble with complicated and non-linear fraud patterns, it works particularly well for binary classification tasks that are typical in fraud detection [28].

B. Unsupervised Machine Learning Algorithms for Fraud Detection

Unsupervised ML algorithms identify unusual patterns and suspicious transactions without requiring labeled fraud data. They are particularly useful for detecting previously unknown fraud by finding anomalies, clusters, and deviations from normal customer behavior.

- **Isolation Forest:** Isolation Forest, which separates data points by picking features at random and then picking split values between the high and low points of those characteristics at random [29]. Outliers, which often indicate fraudulent transactions, are especially easy to spot with its help.
- **Autoencoders:** Discovering latent variables is the job of autoencoders, which are models for latent variables. One part of them, called an encoder, learns to map data X to a low-dimensional latent space Z, while the other part, called a decoder, does the exact opposite, going from Z to the original dimensions.
- **K-Means Clustering:** Each observation is assigned to the cluster that has the closest mean when using K-means clustering [30]. It can identify groups of similar transactions, with those falling outside established clusters potentially representing fraudulent activities.

C. Deep Learning Algorithms for Fraud Detection

DL algorithms use multi-layer neural networks to learn complex patterns from large and high-dimensional financial datasets. They can effectively detect sophisticated fraud by analyzing transaction sequences, customer behavior, and other hidden relationships that traditional methods may overlook.

- **Long Short-Term Memory (LSTM):** LSTM recurrent neural networks employ internal processes called gates to control the flow of input, allowing them to learn long-term data dependencies. LSTM models are able to retain information for long periods of time because these gates can learn which data in a sequence is crucial to preserve or forget.

- **Convolutional Neural Networks (CNNs):** CNNs work well with structured data when it comes to detecting fraud. Essentially, the plan is to use convolutional filters on structured financial data in the same way one would apply a grid to a picture. Their ability to automatically learn hierarchical features from data is extremely important for detecting complicated fraud patterns. Earlier levels of the model catch basic patterns, while deeper layers combine them to uncover more complex associations.
- **Generative Adversarial Networks (GANs):** GANs with competing generator and discriminator networks. For very unbalanced datasets, GANs' ability to produce synthetic fraud samples for use in classifier training makes them an attractive tool for fraud detection [18]. Training instability and "mode collapse," in which the generator outputs a restricted range of samples, are two of the obstacles that GANs confront. Despite its promise for data augmentation, these issues persist.

D. Use Cases Machine Learning in Fraud Detection

ML is widely used to identify suspicious transactions, detect unusual customer behavior, and prevent payment and credit card fraud. Financial organizations can benefit from its real-time analysis of massive amounts of financial data by better spotting new fraud trends [31].

- **Credit Card Fraud Detection:** Credit card fraud may be better detected with the use of collected ML models, which examine trends in spending, the locations of transactions, and previous data. By leveraging anomaly detection techniques, ML algorithms can identify card-not-present (CNP) fraud and unauthorized transactions in real time. The systems use behavioral profiling to compare current transactions against past spending habits, flagging suspicious deviations. Additionally, banks utilize DL models to assess risk scores before approving transactions, reducing false positives and improving security.
- **Identity Theft Prevention:** Fraudsters leverage stolen personal data to create fraudulent accounts, obtain credit, or execute unauthorized transactions. ML models combat these threats by analyzing discrepancies in user-submitted information, geolocation patterns, and behavioral anomalies to flag potential identity theft [32]. These systems continuously adapt to emerging fraud tactics, improving detection of synthetic identities and unauthorized access attempts. Additionally, financial institutions enhance security.
- **Cryptocurrency Fraud Prevention:** Cryptocurrency fraud schemes, such as rug pulls, exploit the anonymity of digital assets. ML models analyze blockchain transaction data to detect fraudulent activities by identifying irregular wallet behavior and suspicious fund movements. Fraud detection systems use clustering algorithms to flag accounts involved in high-risk transactions, helping crypto exchanges prevent illicit activities.

E. Performance Evaluation

The following metrics were used to evaluate the performance of each ML model:

- **Accuracy:** The sum of all the successfully categorized transactions.
- **Precision:** The proportion of anticipated fraudulent transactions that were proved to be true relative to all expected fraudulent transactions. Because it is critical to minimize false positives, this statistic is vital in fraud detection.
- **Recall (Sensitivity):** The proportion of accurately anticipated fraudulent transactions among all fraudulent transactions that actually occur [33]. Make sure the model can identify all fraudulent transactions by using this measure.
- **F1-Score:** A reasonable assessment of the model's performance; the harmonic mean of accuracy and recall.
- **ROC-AUC:** A measure of how well a receiver operates, as seen by the area under the curve that compares the correct and incorrect results. The performance of a model is improved when its AUC is greater.

F. Applications of Machine Learning in Financial Fraud Detection

ML supports diverse financial fraud detection applications by identifying suspicious patterns, reducing risks, and improving transaction security across digital financial services.

- **Credit Card Fraud Detection:** The advances in credit card fraud detection have been radically achieved, going from exploitation of large-scale transactional databases towards the discovery of patterns of behavior, with high probability to be fraudulent [34]. Each ML technique has its strengths and weaknesses, thereby extending the added value to the understanding and addressing the corresponding fraud detection areas.
- **E-Commerce Payment Fraud Detection:** ML offers a wide variety of advanced analytical methods that identify and counteract fraud by spotting unexpected trends, actions, and exceptions [35]. Its dynamic nature allows it to recognize new fraud methods as they develop, guaranteeing effective defense from the various threats.
- **Real-Time Fraud Detection:** The use of ML techniques in handling real-time fraud detection in financial transactions has its advantages and disadvantages. The type of transaction information available, whether labelled data can be obtained, and how important computing efficiency is compared to accuracy of detection is also a factor when deciding on the best technique [36]. The next chapter deals with practical problems and important factors to be taken into consideration when ML solutions are applied to the problem of real-time fraud detection during financial transactions.

G. Challenges in Machine Learning-Based Fraud Detection

Fraud detection based on ML technology encounters difficulties of uneven distribution of data, changing patterns of fraud, amount of labeled data, and occurrence of false positive results. Furthermore, practical problems including data quality, interpretability of models, privacy issues, and necessity for real-time processing lead to unreliability and inefficiency of fraud detection systems.

- **Data Imbalance:** Due to the limited amount of fraudulent transactions present in the entire data, models find it hard to identify important patterns of fraudulent activities.
- **Concept Drift:** The efficiency of models trained on older information is decreased if the trend of fraud changes.
- **Data Privacy and Security:** The training and validation of models cannot occur without the expertise of sensitive financial data [37].
- **Interpretability Issues:** Financial entities usually face difficulties explaining decisions made by complex systems like deep neural networks due to the nature of their work as black boxes.
- **Real-Time Processing Requirements:** The requirement of instant fraud detection means that the models have to be effective and scalable.

IV. LITERATURE REVIEW

The literature discusses various ways of detecting fraud using ML-based technologies, including supervised, unsupervised, ensemble, and DL techniques. Table II provides an overview of important research projects, indicating their methodology, outcomes, shortcomings, and possible future constraints.

K. Prudviraj et al. (2026) There is a proposed AI system that works on the detection of financial fraud by applying ML mechanisms to detect cases of fraud occurring across transactions between people. The proposed system employs a combination of supervised learning, unsupervised anomaly detection, and ensemble techniques for assessing the behavior of transactions. There is an online safe application that helps in the processing of transactions and analyzing and visualizing results. Results of the experiment show improvement in detecting accuracy along with a decrease in false positives compared to traditional systems [38].

Abu Fais Sariat et al. (2025) centered on creating a system that uses ML to identify fraud in mobile money transfers. A synthetic PaySim dataset, sourced from actual bank records, was used in the study. Looked at three different models: XGBoost, LR, and RF. An AUPRC of 0.9998 was the best result attained by RF. Feature engineering, especially with regard to erroneous balance computations, greatly enhanced the ability to identify fraud. Financial transaction systems may be made more safe and dependable with the use of advanced fraud detection technologies [39].

Mritunjay Singh et al. (2024) This system obtains a detection accuracy of 98.5%, a recall of 90.1%, an accuracy of 95.1%, a precision of 92.8%, a recall of 100%, and an F1-score of 91.1 when detecting the query item, according to the experimental study. The results showed that it was successful, as patients' health improved by 2%. In order to maximize the quantity of false positives and negatives for effective antifraud measures, the system learns new kinds of fraud using sequential transaction data [40].

Pratishank Shukla et al. (2023) examines the effectiveness of various ML techniques in detecting and preventing financial fraud associated with transactions. In this study, six different ML methods are examined and contrasted: naive bayes, decision trees, logistic regression, support vector machines, and neural networks. When it comes to identifying suspicious financial transactions, random forest is best bet.

Trends in fraud, including the demographics targeted and the timing of instances, are also shown by the study's data. Future research should aim to investigate more sophisticated ensemble learning techniques, such as DL algorithms, resolve imbalanced datasets, apply real-time fraud detection, and broaden the scope of the study to include other industries, including health [41].

Yinze Yang et al. (2022) Regardless of the amount of time or money invested, the existing method of detecting financial fraud using conventional techniques is labor-intensive and

prone to errors. Yet, new ways to identify financial fraud have emerged thanks to advancements in ML techniques and cloud computing. Several research have looked at using ML models to detect financial fraud, but ML has shown to be the most common approach. If use DL to find financial issues, and can cut costs and improve accuracy. Many supervised and unsupervised learning models have been developed and tested by academics over the last decade to address issues with fraud detection tasks; yet, there is still no conclusive categorization or methodology for financial fraud detection [42].

TABLE II. COMPARATIVE ANALYSIS OF MACHINE LEARNING-BASED FINANCIAL FRAUD DETECTION

Reference	Study Focus	Approach / Methodology	Key Findings	Challenges / Limitations	Future Directions
K. Prudviraj et al. (2026)	AI-based financial fraud detection	Combines supervised learning, unsupervised anomaly detection, and ensemble models for real-time transaction analysis	Improved fraud detection accuracy and reduced false positives compared with traditional methods	Real-time processing and integration of multiple ML approaches may increase system complexity	Develop efficient and scalable real-time fraud detection systems
Abu Fais Sariat et al. (2025)	Fraud detection in mobile money transactions	XGBoost, Logistic Regression, and Random Forest using a PaySim-based dataset	Random Forest achieved an AUPRC of 0.9998; feature engineering improved fraud detection performance	Dataset is based on simulated mobile money transactions	Refine advanced ML methods for secure and reliable financial transactions
Mritunjay Singh et al. (2024)	Real-time financial fraud detection	Successive transaction analysis and learning of emerging fraudulent patterns	Reported high detection performance and supported real-time identification of fraudulent activities	Continuous learning and adaptation to changing fraud patterns remain challenging	Develop adaptive models for evolving fraud patterns and real-time detection
Pratishank Shukla et al. (2023)	Comparative analysis of ML techniques for financial fraud	Naive Bayes, Neural Network, Decision Tree, SVM, Logistic Regression, and Random Forest	Random Forest was identified as the most suitable model for predicting fraudulent transactions	Imbalanced datasets and changing fraud patterns affect detection performance	Explore ensemble and deep learning methods and real-time detection
Yinze Yang et al. (2022)	Review of ML methods for financial fraud detection	Analysis of supervised, unsupervised, and deep learning approaches	ML and deep learning can reduce detection costs and improve fraud detection accuracy	Existing studies lacked comprehensive classification and conclusions	Develop comprehensive and effective ML-based fraud detection frameworks

V. CONCLUSION AND FUTURE WORK

ML is known to be a successful way of detecting fraud. It works by identifying potentially fraudulent transactions, anomalies and changes in customer behavior. Different types of financial fraud were discussed, as well as those factors leading to fraud occurrences. Issues like credit card fraud, financial statement fraud, insurance fraud and internet financial fraud have been assessed. In addition, there are different approaches of ML, such as supervised, unsupervised, and DL approaches, which had been used for financial fraud identification. Nevertheless, problems like dataset imbalance, lack of labelled data, changing nature of fraud, and many others exist.

Future studies should adapt the models continuously learning new fraud patterns in real-time conditions, and thus improve accuracy of its detection. Also, dealing with financial data that is both highly unbalanced and constantly changing is also a matter of future research. The increasing transparency and trust in automated fraud decisions can be achieved through using explainable ML. Therefore, combining ML and DL and real-time monitoring, along with privacy preserving technologies, will increase the effectiveness and reliability of fraud detection systems. Moreover, future studies should examine these methods on various datasets and performance measures to confirm their applicability in practice.

- **Funding:** This research received no external funding.
- **Institutional Review Board Statement:** Not applicable.
- **Informed Consent Statement:** Not applicable.
- **Data Availability Statement:** The data supporting the findings of this study are available from the corresponding author upon reasonable request.
- **Conflicts of Interest:** The author declares no conflict of

How to cite this article:

P. Laxkar, "Machine Learning for Financial Fraud Detection: A Survey of Algorithms and Applications," *Journal of Global Research in Electronics and Communication*, vol. 2, no. 8, pp. 22–28, Aug. 2026. Doi.XXX

REFERENCES

- [1] W. N. Robinson and A. Aria, "Sequential fraud detection for prepaid cards using hidden Markov model divergence," *Expert Syst. Appl.*, vol. 91, pp. 235–251, Jan. 2018, doi: 10.1016/j.eswa.2017.08.043.
- [2] D. Vallarino, "Detecting Financial Fraud with Hybrid Deep Learning: A Mix-of-Experts Approach to Sequential and Anomalous Patterns," *Apr. 2025*, doi: 10.48550/arXiv.2504.03750.
- [3] K. O. Alotaibi, "A Financial Fraud Detection Model Using Artificial Intelligence," *Eng. Technol. Appl. Sci. Res.*, vol. 16, no. 1, pp. 31579–31584, 2026, doi: 10.48084/etasr.15892.
- [4] Y. Pappas, "Fraud Detection Using Machine Learning (Analysis)," 2018.
- [5] R. Palwe, "Adaptive human: AI decision support for high-stakes financial advice," *Int. J. Comput. Artif. Intell.*, vol. 6, no. 2, pp. 385–392, Jul. 2025, doi: 10.33545/27076571.2025.v6.i2e.226.
- [6] H. Verma and M. Sharma, "Rule-Based Hybrid AI – ML Models for Fraud Detection : A Systematic Review and Thematic Analysis," *Int. J. Mod. Sci. Res. Technol.*, vol. 4, no. 1, 2026.
- [7] N. Husnaningtyas and Totok Dewayanto, "Financial Fraud Detection

- and Machine Learning Algorithm (Unsupervised Learning): Systematic Literature Review,” *J. Ris. Akunt. Dan Bisnis Airlangga*, vol. 8, no. 2, pp. 1521–1542, Nov. 2023, doi: 10.20473/jraba.v8i2.49927.
- [8] R. Vishvakarma, “Audit-Ready Explainable Ai For Fraud Operations: Persisted And Replayable Decision Artefacts For Model Governance And Investigator Trust,” *ShodhAI J. Artif. Intell.*, vol. 3, no. 1, pp. 71–78, May 2026, doi: 10.29121/shodhai.v3.i1.2026.77.
- [9] C. S. Pareek, “Testing Approaches In Life Insurance: Accelerated And Fluid Less Underwriting Amidst Data-Driven Dynamics,” *Int. J. Sci. Res. Publ.*, vol. 14, no. 11, pp. 8–10, Nov. 2024, doi: 10.29322/IJSRP.14.11.2024.p15503.
- [10] V. P. Rambabu, J. Sreerama, and J. T. S. Singh, “AI-Driven Data Integration: Enhancing Risk Assessment in the Insurance Industry,” *Aust. J. Mach. Learn. Res. Appl.*, vol. 2, no. 2, pp. 130–179, July, 2022.
- [11] K. Randhawa, C. K. Loo, M. Seera, C. P. Lim, and A. K. Nandi, “Credit Card Fraud Detection Using AdaBoost and Majority Voting,” *IEEE Access*, vol. 6, pp. 14277–14284, 2018, doi: 10.1109/ACCESS.2018.2806420.
- [12] A. Ali *et al.*, “Financial Fraud Detection Based on Machine Learning: A Systematic Literature Review,” *Appl. Sci.*, vol. 12, no. 9, pp. 1–24, September, 2022, doi: 10.3390/app12199637.
- [13] A. Gepp, K. Kumar, and S. Bhattacharya, “Lifting the numbers game: identifying key input variables and a best-performing model to detect financial statement fraud,” *Account. Financ.*, vol. 61, no. 3, pp. 4601–4638, Sep. 2021, doi: 10.1111/acf.12742.
- [14] S. Pawar, G. Patil, K. Patel, P. Pawar, S. Khedkar, and B. More, “Falsified News Detection Using Deep Learning Approach,” in *2021 Asian Conference on Innovation in Technology (ASIANTON)*, PUNE, India: IEEE, Aug. 2021, pp. 1–5. doi: 10.1109/ASIANTON51346.2021.9544585.
- [15] U. I. Usman, M. D. Ibrahim, I. Abdullahi, U. Isah, and F. Jamal, “The Implications of Insider Threats in Financial Institutions: A Review of Challenges and Mitigation Strategies,” *Int. J. Innov. Sci. Res. Technol.*, p. 186, 2025, doi: 10.38124/ijisrt/25dec240.
- [16] W. Syafitri, Z. Shukur, U. Mokhtar, R. Sulaiman, and M. A. Ibrahim, “Social Engineering Attacks Prevention: A Systematic Literature Review,” *IEEE Access*, vol. 10, pp. 39325–39343, 2022, doi: 10.1109/ACCESS.2022.3162594.
- [17] E. R. Allan and D. M. S. Hanspal, “Identity Theft and Online Financial Fraud: Challenges in Enforcement of Cyber Laws in India,” *Int. J. Humanit. Commer. Educ.*, vol. 2, no. 7, pp. 39–45, Jul. 2026, doi: 10.59828/ijhce.v2i7.117.
- [18] H. Tingfei, C. Guangquan, and H. Kuihua, “Using Variational Auto Encoding in Credit Card Fraud Detection,” *IEEE Access*, vol. 8, pp. 149841–149853, 2020, doi: 10.1109/ACCESS.2020.3015600.
- [19] A. Ahsun, S. Oladele, and N. Ratknovic, “The Impact of Emerging Technologies on Traditional Approaches to Financial Fraud Prevention,” *Res. gate*, 2025.
- [20] P. Dubey, P. Dubey, and P. N. Bokoro, “A Unified Transformer–BDI Architecture for Financial Fraud Detection: Distributed Knowledge Transfer Across Diverse Datasets,” *Forecasting*, vol. 7, no. 2, pp. 1–34, 2025, doi: 10.3390/forecast7020031.
- [21] D. Mohanty, V. N. Kumar, C. Patel, T. Manglani, S. Adhav, and N. Sahu, “Implementing Blockchain Technology for Fraud Detection in Financial Management,” vol. 12, p. 2023, 2023.
- [22] Z. Rojan, “Financial Fraud Detection Based on Machine and Deep Learning: A Review,” *Indones. J. Comput. Sci.*, vol. 13, no. 3, Jun. 2024, doi: 10.33022/ijcs.v13i3.4059.
- [23] E. A. Minastireanu and G. Mesnita, “An Analysis of the Most Used Machine Learning Algorithms for Online Fraud Detection,” *Inform. Econ.*, vol. 23, no. 1/2019, pp. 5–16, Mar. 2019, doi: 10.12948/issn14531305/23.1.2019.01.
- [24] H. El Mekki and S. M. Bouaziz, “The Role of Supervised Learning Algorithms in Fraud Detection for Financial Risk Management: A literature review,” Atlantis Press International BV, 2025, pp. 7–19. doi: 10.2991/978-94-6463-892-9_2.
- [25] A. A. Compagnino *et al.*, “An Introduction to Machine Learning Methods for Fraud Detection,” *Appl. Sci.*, vol. 15, no. 21, p. 11787, Nov. 2025, doi: 10.3390/app15211787.
- [26] A. Ahirwar, N. Sharma, and A. Bano, “Enhanced SMOTE & fast random forest techniques for credit card fraud detection,” *Solid State Technol.*, vol. 63, no. 6, pp. 4721–4733, 2020.
- [27] A. Pagliaro, “Forecasting Significant Stock Market Price Changes Using Machine Learning: Extra Trees Classifier Leads,” *Electron.*, vol. 12, no. 21, pp. 1–23, 2023, doi: 10.3390/electronics12214551.
- [28] W. W. Soh and R. M. Yusuf, “Predicting Credit Card Fraud on a Imbalanced Data,” *Int. J. Data Sci. Adv. Anal.*, vol. 1, no. 1, pp. 12–17, 2019, doi: 10.69511/ijdsaa.v1i1.3.
- [29] V. Vijayakumar, N. S. Divya, P. Sarojini, and K. Sonika, “Isolation Forest and Local Outlier Factor for Credit Card Fraud Detection System,” *Int. J. Eng. Adv. Technol.*, vol. 9, no. 4, pp. 261–265, 2020, doi: 10.35940/ijeat.d6815.049420.
- [30] S. Subudhi and S. Panigrahi, “Use of optimized Fuzzy C-Means clustering and supervised classifiers for automobile insurance fraud detection,” *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 32, no. 5, pp. 568–575, 2020, doi: 10.1016/j.jksuci.2017.09.010.
- [31] S. Singh, S. A. Pahune, P. Chatterjee, and R. Sura, “Advanced Machine Learning Methods for Churn Prediction and Classification in Telecom Sector,” in *2025 IEEE 6th India Council International Subsections Conference (INDISCON)*, Rourkela, India: IEEE, 2025, pp. 1–7, December. doi: 10.1109/INDISCON66021.2025.11252233.
- [32] K. Srinivasa, Vangibhurathachhi, and S. K. Vangibhurathachhi, “Machine Learning for Fraud Detection in Financial Transactions,” 2025. doi: 10.13140/RG.2.2.24887.23200.
- [33] M. Inairat, N. A. Hamza, R. Hamdy Abdalhamid, S. AlShuweih, S. Salloum, and S. K. Alokdeh, “Machine Learning for Fraud Detection in Financial Transactions,” in *2025 International Conference on Business Intelligence for Technology Innovation (ICBITI)*, IEEE, Apr. 2025, pp. 1–7. doi: 10.1109/ICBITI65527.2025.11500679.
- [34] P. K. P. Chunawala, “A Review On Credit Card Fraud Detection Using Machine Learning,” *Int. J. Sci. Technol. Res.*, vol. 8, no. 10, pp. 1217–1220, 2024, doi: 10.2139/ssrn.4982335.
- [35] A. Narayan, S. D. Madhu Kumar, and A. M. Chacko, “A Review of Financial Fraud Detection in E-Commerce Using Machine Learning,” in *Smart Innovation, Systems and Technologies*, vol. 327, 2023, pp. 237–248. doi: 10.1007/978-981-19-7524-0_21.
- [36] M. A. Mohammed, K. R. V. Kothapalli, R. Mohammed, P. Pasam, D. K. Sachani, and N. Richardson, “Machine Learning-Based Real-Time Fraud Detection in Financial Transactions,” *Asian Account. Audit. Adv.*, vol. 8, pp. 67–76, 2017.
- [37] R. Jeyaraj, N. A. Natraj, M. P. Rajasekaran, and K. Gangadharan, “Machine Learning Techniques for Fraud Detection in Financial Services,” *Int. J. Adv. IT Res. Dev.*, vol. 01, no. 01, 2024, doi: 10.69942/1920184/20240101/04.
- [38] K. Prudviraj, G. Q. Hannah, B. Nivedhitha, M. Sireesha, K. Shilpa, and G. P. Kumar, “Comparative Analysis of Machine Learning Algorithms for Financial Fraud Detection,” in *2026 International Conference on Machine Learning and Autonomous Systems (ICMLAS)*, 2026, pp. 665–671. doi: 10.1109/ICMLAS67792.2026.11483932.
- [39] A. F. Sariat, I. J. Siddique, M. Hossain, M. M. Islam, and T. Rahman, “AI Driven Fraud Detection in Financial Ecosystems: A Hybrid Machine Learning Framework,” in *2025 International Conference on Electrical, Computer and Communication Engineering (ECCE)*, 2025, pp. 1–8. doi: 10.1109/ECCE64574.2025.11013808.
- [40] M. Singh, N. Bansal, G. S. K. Kavithamani, M. Almusawi, and C. P. Patnaik, “Real-Time Fraud Detection in Financial Transactions Using Autoencoders,” in *2024 International Conference on Advances in Computing, Communication and Materials (ICACCM)*, 2024, pp. 1–4. doi: 10.1109/ICACCM61117.2024.11058990.
- [41] P. Shukla, M. Aggarwal, P. Jain, P. Khanna, and M. K. Rana, “Financial Fraud Detection and Comparison Using Different Machine Learning Techniques,” in *2023 3rd International Conference on Technological Advancements in Computational Sciences (ICTACS)*, 2023, pp. 1205–1210. doi: 10.1109/ICTACS59847.2023.10390165.
- [42] Y. Yang, Y. Yu, and T. Li, “Deep Learning Techniques for Financial Fraud Detection,” in *2022 14th International Conference on Computer Research and Development (ICCRD)*, 2022, pp. 16–22. doi: 10.1109/ICCRD54409.2022.9730314.