ISSN 2581 – 3781

Available Online at www.ajcse.info
Asian Journal of Computer Science Engineering 2025;10(3)

REVIEW ARTICLE

Machine Learning for Credit and Transaction Risk Scoring Mitigation in Financial Frauds: A Review

Sreenivasulu Gajula*,
Principal Full-Stack Engineer
Sreenivasgajulausa@gmail.com

Siva Teja Reddy Kandula
Software Developer
sivateja.kandula@ieee.org

***Abstract*—Financial fraud remains a pervasive challenge in the global financial market, causing substantial economic losses and undermining trust in financial institutions. In addition to outlining several fraud categories, such as credit card fraud, financial statement fraud, insurance fraud, mortgage fraud, and money laundering, this paper offers a thorough review of financial fraud with an emphasis on credit and transaction risk. It examines the fundamental ideas of credit and transaction risks, such as counterparty, concentration, nation, default, and settlement risks, and highlights how important machine learning methods are to improving risk assessment and fraud detection. The study looks at state-of-the-art methods for effectively identifying and reducing fraudulent behavior, including deep learning architectures, neural networks, decision trees, support vector machines, and supervised and unsupervised learning. Furthermore, it discusses integrated fraud detection frameworks that leverage multimodal data fusion, unified risk assessment, and real-time adaptive scoring to improve detection accuracy and operational efficiency. The study concludes by identifying emerging trends and future research directions to strengthen financial fraud prevention and risk management in an increasingly digital financial ecosystem.**

Keywords*— Machine Learning, Transaction Risk Scoring, Financial Frauds, Credit Score, Mitigation Strategies.

INTRODUCTION

Organizations, the financial industry and individuals worldwide continue to face the main challenge of financial fraud in the global financial market. Annually, fraud cost the United States economy billions of dollars in losses [1][2]. This lowers the trust people have in financial companies, pushes markets into disorder and reduces consumer confidence. Credit card fraud is one kind of financial fraud, but there are others as well [3], tax evasion, financial statement manipulation, and money laundering. Numerous analysts concur that fraud falls into one of two categories: banking, insurance and corporate types and each has its specific problems and outcomes [4]. As services move online, it is becoming easier for unethical individuals to use new ways to commit digital fraud.

One of the most prevalent and harmful issues associated with cybercrime nowadays is credit card theft [5][6]. The use of internet payment applications is growing, making contactless purchases and mobile banking have given rise to new ways for fraudsters to act [7][8]. Conventional fraud detection methods and models for credit card use usually do not keep up with new ways fraudsters are working. Because these systems mostly focus on well-known fraud, they cannot catch fresh or discreet fraud cases in real time which may cause harm to consumers and the financial system. The fact that real transactions far outnumber fraudulent transactions in most datasets makes it hard for common detection methods to identify fraud. As a result, systems must be able to understand and adapt to huge and complicated sets of transactional data.

Financial organisations are thus utilizing ML more often to enhance their defenses against fraud and to determine how risky specific actions are. Transaction data from many sources is efficiently processed by ML models to spot anomalies, assess the risks and predict possible fraud [9][10]. In learning about the complex patterns and connections in transaction data, DL, ensemble learning, anomaly detection, and supervised and unsupervised learning have all shown great promise [11][12]. These models make it possible to detect fraud now and help create predictive scoring systems, useful for noticing if new fraud is likely, so companies can take preventive measures. Such designs are able to update themselves to stay ahead of new fraud trends, giving them more scalability and stability than older systems.

Structure of the Paper

The structure of this paper is as follows: **Section II** outlines the foundations of credit and transaction risk in financial fraud. **Section III** reviews risk scoring techniques used for fraud detection. **Section IV** discusses mitigation strategies and integrated fraud detection frameworks. **Section V** presents a literature review of recent ML approaches. **Section VI** brings the work to a close and makes recommendations for further research.

Foundations Of Credit And Transaction Risk In Financial Fraud

Almost 20 years after the Enron scandal, financial fraud is still a problem, even with laws like the Sarbanes-Oxley Act and the creation of the PCAOB to improve auditing. Well-known investors, like the “Oracle of Omaha,” have also been affected by fraud. To fight this, experts suggest using financial insurance and new tools like blockchain to make transactions more secure. Still, detecting financial statement fraud is difficult. The SEC says 50% of fraud cases involve false revenue reporting, 35% involve hiding debts or costs, and the rest come from missing information in footnotes. The attention on financial fraud has significantly increased over the past ten years due to the potential effects of undetected abnormalities on the industry and day-to-day living. These crimes can take many various forms, and they can destabilize economies, increase living expenses, and reduce consumer trust [13][14]. Financial fraud is defined by the ACFE as "any intentional or deliberate act to deprive another of property or money by guile, deception, or other unfair means," although there isn't a single, generally accepted definition available.

Types of Financial Frauds

There are several kinds of financial fraud. Regarding the harm these crimes provide to the economy, however, a few prominent names include money laundering, insurance fraud, credit card fraud, and financial statement fraud. In Fig. 1, a categorization is shown. The following is a quick description of them.

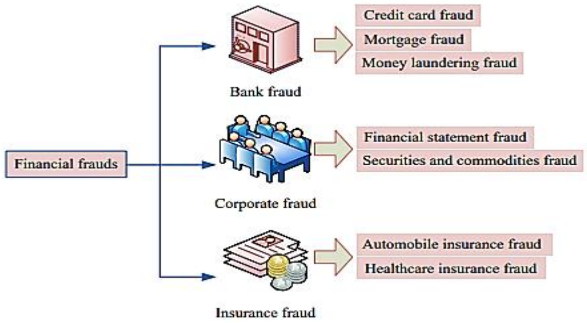
Financial frauds
Bank fraud
Credit card fraud
Mortgage fraud
Money laundering fraud
Corporate fraud
Financial statement fraud
Securities and commodities fraud
Insurance fraud
Automobile insurance fraud
Healthcare insurance fraud

Fig. 1. Type of Financial Frauds

- **Credit Card Fraud:** The term "bank fraud" usually refers to credit card fraud. Credit card fraud is generally defined as the unauthorized use and access of a person's credit card without that person's consent or knowledge. Credit card fraud falls into two groups. The first one has a bunch of scammers carrying out the scam. We call this kind of credit card theft "counterfeit fraud." Ten to hundreds of a bank's cardholders may be impacted by this conduct, which has enormous consequences.
- **Financial Statement Fraud:** A company's financial statements are collections of information on its cash flows and overall financial health, costs, loans, earnings, and other financial information [15]. accompanied by some remarks and suggestions on the company and anticipated future business challenges from the management.
- **Insurance Fraud:** Insurance fraud is any action taken with the false aim to obtain a fraudulent payout from an insurance provider. This kind of fraud can occur at any point in the insurance process (such as during application, rating, eligibility, billing, claims, etc.), and it can be perpetrated by brokers, consumer agents, insurance company staff, and others.
- **Mortgage Fraud:** The goal of mortgage fraud is to significantly falsify or omit information on a mortgage loan application in order to get a loan or gain financial benefit that would not have been possible had the borrower known the truth.
- **Money Laundering:** A type of financial fraud known as "money laundering" occurs when a scammer attempts to pass off illicit or filthy funds as clean or legal funds [15].

Credit and Transaction Risk: Concepts and Types

As this risk can determine the success or failure of financial institutions, it is vital in lending, investing and financial dealings. It often comes from places such as consumers, businesses or whole governments. To do credit risk management well, must judge how likely it is for someone to be unable to pay back and estimate the amount that would be lost if that happens. Conventional assessments of credit risks depend on information such as management, public image and financial and statistical data [16]. Nowadays, experts use ML, neural networks and similar methods to make credit risk prediction both more accurate and efficient. They examine different data to look for warning signs of upcoming defaults. Thanks to strong credit risk knowledge, financial institutions are better placed to approve loans with confidence, set suitable loan rates, use funds wisely and remain in line with regulations.

- **Default Risk:** It represents the fundamental kind of credit risk. It happens when a borrower fails to make principle or interest payments on time. Banks and investors in bonds, as well as any lenders, feel the effects of default risk. How much this type of risk matters is based on the credit score and rating of the borrower.
- **Counterparty Risk:** A situation in derivative markets, trading or securities financing, counterparty risk occurs if the other party to a transaction (such as a swap, futures or repurchase agreement) does not carry out their part of the agreement. In contrast to traditional lending, this risk affects OTC transactions more commonly because there is no central clearinghouse involved.
- **Concentration Risk:** The problem results from being overly exposed to just one borrower, one sector or one location. A failure by one particular entity or group may increase losses, as there is not enough variety in the portfolio. They achieve this by confirming their maximum exposures and ensure their portfolios are not too reliant on one type of investment.
- **Country or Sovereign Risk:** It describes the possibility that either the government or some sectors inside a country may default because of instability, economic decline, problems with currency or new government policies. A country’s default among sovereign debt obligations can influence international banks, investors and exporters linked to the struggling country.
- **Settlement Risk:** If one side pays but the other does not exchange what is agreed upon, it is called settlement risk. It becomes very important in foreign exchange and securities trading since settlements might happen at various times or in different places.

Credit and Transaction Risk

This emphasizes the risk of credit and transactions as well as the fundamental concepts discussed:

1) Credit Risk Fundamentals

Credit risk occurs when a lender or institution faces the chance of losing money because a borrower does not pay back the loan or meet the terms they agreed to. Credit risk happens in lending, bond markets, with credit cards and when dealing with derivatives and it is normally evaluated based on the likelihood of defaults [17]. To assess credit risk, one should analyze both factors related to the borrower and to the economy as a whole. The process of assessing credit may include methods that are qualitative or models that use logistic regression, neural networking or other such group techniques [18][19]. Estimating and grouping default risk for individuals and companies is made possible through credit scoring and credit rating systems. Strong credit risk management, using different methods, limits and advanced models, secures financial stability and meets rules set by regulators.

2) Transaction Risk Categories

Transaction risk is caused by issues or weaknesses in the ways financial transactions are carried out. It means there is a chance of losing money from errors, fraud, problems with the financial system or delays during handling transactions [20]. Dealing with financial fraud, it's important to focus on transaction risk due to the chance of suspicious movements within the transfer and payment systems. Among the main types of transaction risk are:

- **Operational Risk:** Often comes from poorly designed or broken internal processes, staff or systems. Examples range from technical problems, to mistakes by people or errors in carrying out transactions.
- **Fraud Risk:** It means users have their identity or money taken without consent in various forms. This issue is very important in the world of online and card payments.
- **Settlement Risk:** The situation arises when one party in a transaction provides what they agreed to but the other doesn't follow through [21]. A usual practice in both foreign exchange and securities trading.
- **Systemic Risk:** Offers coverage for larger problems in the financial system that could interrupt processing transactions [22], often because of worry in the market, cyber-attacks or financial pandemics [23][24].
- **Compliance and Regulatory Risk:** Failing to match AML or KYC requirements when transacting may lead to the trades being held up or partially reversed which can result in lawsuits.

Risk Scoring Techniques For Credit And Transaction

Considering its strategic, financial, and regulatory significance, credit risk assessment is crucial for banks and other financial organisations. Central banks and auditors are among the regulatory agencies that regularly monitor adherence to Basel and IFRS standards [21][25]. Accurate scoring ensures profitability, overestimating risk can lead to overpriced loans and lost customers; while underestimating it may cause financial losses. Additionally, credit risk scores can support decision-making in client services, such as recommendation systems and marketing strategies.

Machine Learning Approaches in Credit Scoring

The capacity of ML to analyses vast and intricate data sets to provide more accurate predictions has enhanced credit risk scoring. SVM and ANN were initially more successful than LR because they were able to comprehend the intricate, curved patterns included in credit data. The predictions of these models were dependable, yet their unclear processes caused problems for regulation.

Recently, using RF and GBM has become more common as people appreciate that they combine different classifiers for a better outcome [26]. Widespread adoption of XGBoost comes from its strength, the capability to manage a lot of data and its sturdiness in data handling. Because of its ease of use, lenders now turn to credit scoring to quickly flag borrowers who might default.

The main difficulty with ML is its lack of interpretability. It is easy for regulators to accept transparent models like logistic regression, but to consider complex models like GBMs and DL [27], AI must be explainable. Systems such as SHAP have been created to boost the clarity of models, enabling institutions to see the impact of each component on credit decisions. Such approaches ensure that regulation is followed while using advanced ML for credit scoring.

Transaction Risk Scoring Techniques

Transaction Risk Scoring is a technique for assessing the risk involved in a certain transaction [28]. It determines a risk score by analyzing several data points and patterns, which indicates the likelihood that the transaction is fraudulent. The score influences businesses to accept, review or reject a transaction. There are a few steps to transaction risk scoring:

- **Data Collection:** The ability to collect information from multiple sources like transaction details, user behaviour, device information and so forth.
- **Analysis:** Algorithms and ML models are used to analyze the collected data using algorithms and ML models.
- **Scoring:** Dynamically assigning a risk score based on the analysis of the transaction that shows the probability of being fraudulent.
- **Decision Making:** The risk score helps to make decisions on the transaction.

3) The Importance of Transaction Risk Scoring in Payment Processing

a) Fraud Prevention

The primary reason for transaction risk scoring is to stop fraud. With the ability to identify high-risk transactions, businesses can take proactive measures to prevent fraudulent activities, thus protecting revenue and reputation.

b) Enhancing Customer Experience

Preventing fraud is important, but so is providing a smooth, no-hassle customer experience for valid customers. Transaction risk scoring achieves a balance between accepting transactions and rejecting them by accurately determining which transactions are genuine and which are fraudulent and in doing so, it reduces false positives, increasing customer satisfaction.

c) Cost Efficiency

Transaction risk scoring can realize very significant cost savings. The reduction of fraudulent transactions can lead businesses to save money on chargeback fees, penalties and other costs. Besides, automated risk scoring systems decrease the need for manual review; due to this, operational costs decreased.

Mitigation Strategies And Integrated Fraud Detection Frameworks

This section focusses on system integration and grading for actionable fraud reduction.

Artificial Intelligence Techniques in Fraud Detection

4) Supervised and Unsupervised Learning Methods

The use of ML techniques, which are divided into supervised and unsupervised learning, has significantly contributed to the current revolution in fraud detection brought about by AI. One of the most popular methods is supervised learning, which involves using a labelled dataset to train a model. Each occurrence of the dataset has an associated result, often whether or not a transaction is fraudulent [29][30]. The model may then learn to accurately predict the class of fresh, unknown data by learning these correlations between input properties and their labels. Fraud detection makes extensive use of supervised learning models, such as logistic regression, random forests, and SVM [31], as they are easy to interpret and effective with structured data.

In the other case, unsupervised learning techniques are applied when the labeled data is rare or unavailable. In unsupervised fraud detection, the model becomes a pattern, anomaly or outlier detection model without any previous information about what fraud is particular, this method works well for identifying new fraud strategies that deviate from established trends [32]. Commonly used algorithms for clustering include K-means and DBSCAN, and anomaly detection techniques include forest to uncover Behavior that is considered anomalous based on some deviation from the normal trend. These techniques look at departures from normal transaction patterns to identify undiscovered fraud schemes rather than depending on preset fraud labels.

5) *Neural Networks, Decision Trees, Support Vector Machines*

Several ML approaches, including neural networks, decision trees, and SVM, are frequently employed to detect fraud and are particularly useful because of their flexibility and ability to learn nonlinear relationships in the data that are used to model financial data.

Fraud Detection using Neural Networks, especially DNN, has become increasingly popular for learning hierarchical feature representations from raw data. Neural Networks have DL architecture, which means that they don't require manually created feature engineering since they can automatically extract valuable features from incoming data. Fraud detection is one such example where fraud patterns are intricate and hard to identify by conventional means, and this is particularly valuable.

The DT which are a more interpretable way to detect fraud. These models take input data and split it into decision nodes according to feature values, and eventually reaching a decision on whether a transaction is fraudulent or legitimate. For fraud detection, DT are often built using such algorithms as CART (Classification and Regression Trees) and C4.5. They have an advantage: clear rules for how to make decisions which can be important to understand why certain transactions get flagged.

In fraud detection, SVM are another powerful tool, particularly for binary classification tasks like the differentiation between fraudulent and legitimate transactions [33]. Machine algorithms operate by determining the optimal hyperplane in the feature space that divides classes with the greatest distance (margin). SVM's however, have the ability to paint on high-dimensional data and model nonlinear decision boundaries, especially with the kernel trick, which makes them highly effective in complex fraud detection environments.

6) *Deep Learning Approaches for Pattern Recognition*

There has been a major shift to DL techniques (which are a subset of ML that includes training multilayer neural networks) for fraud detection [34], particularly for detecting fraud in applications that handle substantial volumes of unstructured or semi-structured data. DL approaches are great at learning complex patterns and detecting anomalies for which traditional models may fail. In particular, if transaction sequences or temporal dependencies are important in fraud detection, CNN can be adapted for financial data analysis as they have proven to perform exceptionally well in image and sequence data [35]. RNNs, including LSTM networks, are very helpful for identifying patterns that point to fraudulent activity in time-series data, such as transaction sequences.

Integrated Risk Scoring and Decision System

In the face of rising sophistication of financial fraud, financial institutions are increasingly resorting to integrated approaches to the evaluation of risk [36]. Modern systems, instead, try to combine the various risk indicators in one single framework, rather than considering separately credit and behavioral risks. Data analytics, ML and real-time monitoring are based upon to get a detailed and accurate view of a customer's risk profile. It allows for swift and better-informed decision-making as well as better fraud detection capabilities.

7) *Unified Risk Assessment Frameworks*

The unified risk assessment framework is a combination of multiple risk domains (e.g., credit risk, fraud risk, compliance risk) in a single structure of evaluation. These frameworks allow institutions to evaluate a customer's complete risk posture by, e.g., evaluating credit history, transaction Behavior, device fingerprints and geolocation data. Integrating siloed risk models can also improve consistency in risk evaluations among departments as well as reduce duplication of efforts. In addition, unified frameworks also support regulatory compliance by supporting traceable and explainable decision-making processes.

8) *Multimodal Data Fusion*

It is well recognized that semi-structured (like clickstream logs), unstructured (like social media, text from customer interactions), and structured (like credit scores, income data) data may all be integrated. Multimodal data fusion that increases the precision of risk rating. It helps financial systems have a more complete customer profile and to detect anomalies that might not be detectable with single-source data. Processing and fusing these heterogeneous data sources often require techniques such as feature engineering, DL and ensemble methods, which improve on predictive power and early risk detection.

9) *Real-Time Scoring and Adaptive Mitigation*

Real-time scoring systems continuously monitor transactions and customer behavior to give dynamic risk evaluations. Institutions can take proactive actions on these systems such as flagging suspicious activity or adjusting credit limits based upon evolving risk patterns due to the fact that these systems can handle massive amounts of data in real time. AI and ML–driven adaptive mitigation techniques automatically adapt thresholds and response strategies as the severity and context of the risk change. Therefore, it facilitates prompt action and narrows the window of opportunity for scammers.

Literature Review

The existing research in AI and ML in financial fraud detection has been largely focused on improving the risk score accuracy. DL models have been integrated to more effective capture complex fraud patterns and adaptive frameworks for real-time mitigation of risk, and predictive fraud prevention has been developed:

Roshini et al. (2025) This analysis focuses on dealing with this critical issue by establishing a model developed on ML that can identify fraudulent transactions effectively. Developed model leverages earlier credit card transactions to identify patterns indicative of fraud. By employing several kinds of ML algorithms, comprising KNN, LR, RF, DT, and XGB Classifier, the project evaluates the performance of each approach in accurately differentiating between transactions that are fraudulent and those that are not. These models work well for preventing credit card scams as they can manage unbalanced data, identify irregularities, and adjust to intricate fraud patterns [37].

Hemanth et al. (2025) this study presents the real-world credit card transactions with a great class imbalance (i.e. the number of frauds is far lower than that for normal activities) are used as a training data set. This is handled by steps like data preprocessing, normalization, encoding and sampling techniques intended to make the model robust: (i. e., more accurate). EDA, Since we can conduct our EDA on this dataset to see the overall pattern, which will be valuable in identifying what features are most important for fraudulent behavior [38].

Kesharwani and Shukla (2024) To get over these challenges, present a state-of-the-art fraud detection method that makes use of Graph Neural Networks (GNN). Our model synergistically combines the strengths of graph-based learning with deep neural networks to effectively capture the complex relationships and patterns inherent in financial transactions. By utilizing a multi-layered approach, our GNN model not only identifies anomalous patterns indicative of fraud but also adapts to evolving fraudulent tactics. A key feature of our model is the integration of node and edge features, which enhances the representation of transaction networks [39].

Marripudugala (2024) explores various fraud types, such as payment fraud and account takeover fraud, demonstrating the importance of the estimated $343 billion in online payment theft by 2027. We go over fraud detection techniques, including ML, behavioral analytics, anomaly detection, and data analytics. We tested three ML models: MLP, DT, and LR, using a synthetic dataset of mobile money transactions. The DT demonstrated balanced performance with superior precision and recall, but LR had trouble with unbalanced data. Despite its accuracy, the MLP's recall was poor, and it failed to detect important fraud incidents. These results highlight the necessity of optimizing models for efficient fraud detection [40].

Abbas et al. (2024) This study's main goals are to gather the corpus of existing research, identify knowledge gaps, and suggest future lines of inquiry. Using the systematic literature review (SLR) approach, the study carefully reviews relevant primary literature to determine which algorithms for ML work best for fraud detection. The evaluation cautiously selects research from numerous databases, highlighting ML promise and ability to detect fraud in financial statements. Results indicate that by identifying complicated patterns and irregularities that traditional approaches can overlook, advanced ML techniques, particularly DL methods and ensemble learning models, significantly increase the accuracy of fraudulent activity identification [41].

Jesus et al. (2023) The purpose of this study is to determine the benefits of financial institutions using OSINT and how the present Open Finance and LGPD processes may help classify client scores in the best possible way in order to reduce risks and fraud and improve decision-making efficiency. A macro model was suggested as a first outcome of the agreed blueprint to assist financial institutions in validating their own models. The chosen example generates €100,000.00 (one hundred thousand euros) in volume per day on average [42].

The comparative analysis of the background study based on its author(s), Objectives, methods, key findings, contributions, limitations, and future work is provided in Table I.

TABLE I. SUMMARY OF LITERATURE REVIEW BASED ON CREDIT AND TRANSACTION RISK IN FINANCIAL FRAUDS

Author(s)	Objectives	Methods	Key Findings	Contributions	Limitations	Future Work
Roshini et al. (2025)	Develop ML-based model to detect fraudulent credit card transactions	XGB Classifier, Random Forest, KNN, Logistic Regression, and Decision Trees	ML models effectively identify fraud, handle imbalanced data, and detect complex fraud patterns	Demonstrated comparative performance of multiple ML algorithms	Limited to earlier transaction data; may lack real-time adaptability	Expand model for real-time detection and additional datasets
Hemanth et al. (2025)	Improve fraud detection accuracy on highly imbalanced datasets	Data preprocessing, normalization, encoding, sampling, Exploratory Data Analysis (EDA)	EDA identifies important fraud indicators; preprocessing improves robustness and accuracy	Strong preprocessing pipeline and insight into feature importance	Focused on imbalanced data; model comparison not emphasized	Test additional models and automation of feature selection
Kesharwani & Shukla (2024)	Detect fraud using graph-based deep learning	Graph Neural Networks (GNN) with node and edge feature integration	GNN effectively captures complex relationships in transaction data; adapts to new fraud tactics	Introduces GNN-based hybrid model for fraud detection	Computational complexity and lack of interpretability	Optimize performance and explore real-world deployment
Marripudugala (2024)	Compare methods for detecting fraud in mobile money transfers	Multi-layer perceptron's (MLPs), logistic regression, and decision trees on synthetic data	Decision Tree showed best balance; Logistic Regression poor with imbalance; MLP precise but low recall	Highlights challenges of imbalanced data and model tuning	Synthetic dataset limits generalizability	Apply to real datasets and optimize precision-recall balance
Abbas et al. (2024)	Conduct SLR to identify best ML algorithms for fraud detection	Systematic Literature Review (SLR) of primary studies from major databases	Deep learning and ensemble models significantly outperform traditional techniques	Provides synthesis of current ML practices in financial fraud detection	Does not present new model; focused on review	Identify underexplored algorithms and benchmark new hybrid models
Jesus et al. (2023)	Explore use of OSINT and Open Finance mechanisms to mitigate fraud	Macro-model design; Open-Source Intelligence (OSINT); Open Finance data and LGPD framework	Proposed model helps institutions validate customer risk and fraud scores	Incorporates regulatory frameworks with OSINT for decision support	Limited details on model validation; case-specific	Broaden to multiple financial contexts and evaluate scalability

Conclusion And Future Scope

As per the data transactions are made online, credit card fraud continues to be a growing problem. The global financial ecosystem is still at risk from financial fraud, which necessitates sophisticated and flexible detection and mitigation techniques. The importance of AI and ML in improving credit and transaction risk assessment has been emphasized in this study, allowing for the quicker and more precise detection of fraudulent activity. By offering a thorough understanding of risk and facilitating proactive decision-making, the integration of various data sources and real-time risk scoring systems enhances efforts to avoid fraud. In order to meet regulatory requirements, future research should concentrate on making complex models easier to understand, investigating more advanced multimodal data fusion techniques, and creating resilient adaptive systems that can react to new fraud trends in ever-changing financial environments. Additionally, leveraging advancements in explainable AI and privacy-preserving machine learning could pave the way for more transparent, secure, and effective fraud detection solutions.

References

[1] A. Singh, A. Jain, and S. E. Biable, “Financial Fraud Detection Approach Based on Firefly Optimization Algorithm and Support Vector Machine,” *Appl. Comput. Intell. Soft Comput.*, vol. 2022, pp. 1–10, Jun. 2022, doi: 10.1155/2022/1468015.

[2] N. Malali, “AI Ethics in Financial Services: A Global Perspective,” *Int. J. Innov. Sci. Res. Technol.*, vol. 10, no. 2, pp. 2456–2165, 2025, doi: /10.5281/zenodo.14881349.

[3] J. K. Chaudhary, S. Tyagi, H. P. Sharma, S. V. Akram, D. R. Sisodia, and D. Kapila, “Machine Learning Model-Based Financial Market Sentiment Prediction and Application,” in *2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)*, IEEE, May 2023, pp. 1456–1459. doi: 10.1109/ICACITE57410.2023.10183344.

[4] A. Reurink, “Financial Fraud: A Literature Review,” *J. Econ. Surv.*, vol. 32, no. 5, pp. 1292–1325, Dec. 2018, doi: 10.1111/joes.12294.

[5] V. Prajapati, “Enhancing Threat Intelligence and Cyber Defense through Big Data Analytics : A Review Study,” *J. Glob. Res. Math. Arch.*, vol. 12, no. 4, pp. 1–6, 2025.

[6] D. Rao, “Implications of Cyber-Physical Adversarial Attacks on Autonomous Systems,” *Int. J. Exp. Res. Rev.*, vol. 46, p. Pages, 2024.

[7] P. Jha, S. Srivastava, T. Gandhi, and G. P, “Financial Fraud Detection for Credit Card Transactions Using Apache Spark,” in *2024 International Conference on Sustainable Communication Networks and Application (ICSCNA)*, IEEE, Dec. 2024, pp. 427–431. doi: 10.1109/ICSCNA63714.2024.10864321.

[8] S. J. Wawge, “A Survey on the Identification of Credit Card Fraud Using Machine Learning with Precision, Performance, and Challenges,” *Int. J. Innov. Sci. Res. Technol.*, vol. 10, no. 4, pp. 3345–3352, May 2025, doi: 10.38124/ijisrt/25apr1813.

[9] R. C. D. Morán *et al.*, “Application of Machine Learning Models in Fraud Detection in Financial Transactions,” *Data Metadata*, vol. 2, p. 109, Oct. 2023, doi: 10.56294/dm2023109.

[10] N. Prajapati, “The Role of Machine Learning in Big Data Analytics: Tools, Techniques, and Applications,” *ESP J. Eng. Technol. Adv.*, vol. 5, no. 2, pp. 16–22, 2025, doi: 10.56472/25832646/JETA-V5I2P103.

[11] A. Balasubramanian, “Personalized Career Pathway: A Hybrid Machine Learning Approach for Dynamic Recommendations,” *J Artif Intell Mach Learn Data Sci 2023*, vol. 1, no. 4, pp. 1999–2003, 2023.

[12] S. Wawge, “Evaluating Machine Learning and Deep Learning Models for Housing Price Prediction,” *IJARSCT*, vol. 5, no. 11, pp. 367–377, 2025.

[13] W. Hilal, S. A. Gadsden, and J. Yawney, “Financial Fraud: A Review of Anomaly Detection Techniques and Recent Advances,” 2022. doi: 10.1016/j.eswa.2021.116429.

[14] A. Balasubramanian and N. Gurushankar, “Building Secure Cybersecurity Infrastructure: Integrating AI and Hardware for Real-Time Threat Analysis,” *Int. J. Core Eng. Manag.*, vol. 6, no. 7, 2020.

[15] M. N. Ashtiani and B. Raahemi, “Intelligent Fraud Detection in Financial Statements Using Machine Learning and Data Mining: A Systematic Literature Review,” *IEEE Access*, vol. 10, pp. 72504–72525, 2022, doi: 10.1109/ACCESS.2021.3096799.

[16] B. Ramanujam, “Statistical in Sights in to Anti-Money Laundering : Analyzing Large-Scale Financial Transactions,” *Int. J. Eng. Res. Technol.*, vol. 14, no. 04, 2025, doi: 10.17577/IJERTV14IS040136.

[17] S. Tyagi, “Analyzing Machine Learning Models for Credit Scoring with Explainable AI and Optimizing Investment Decisions,” *Am. Int. J. Bus. Manag.*, vol. 5, no. 01, pp. 5–19, 2022.

[18] N. Chen, B. Ribeiro, and A. Chen, “Financial credit risk assessment: a recent review,” *Artif. Intell. Rev.*, 2016, doi: 10.1007/s10462-015-9434-x.

[19] N. Prajapati, “Federated Learning for Privacy-Preserving Cybersecurity : A Review on Secure Threat Detection,” *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 5, no. 4, pp. 520–528, 2025, doi: 10.48175/IJARSCT-25168.

[20] S. Zamore, K. Ohene Djan, I. Alon, and B. Hobdari, “Credit Risk Research: Review and Agenda,” 2018. doi: 10.1080/1540496X.2018.1433658.

[21] A. Markov, Z. Seleznyova, and V. Lapshin, “Credit scoring methods: Latest trends and points to consider,” *J. Financ. Data Sci.*, vol. 8, pp. 180–201, 2022, doi: 10.1016/j.jfds.2022.07.002.

[22] E. Xhumari and S. Haloci, “A comparative study of Credit Scoring and Risk Management Techniques in Fintech: Machine Learning vs. Regression Analysis,” *CEUR Workshop Proc.*, vol. 3402, pp. 13–20, 2023.

[23] S. Singamsetty, “Fuzzy-Optimized Lightweight Cyber-Attack Detection for Secure Edge-Based IoT,” *J. Crit. Rev.*, vol. 6, no. 07, pp. 1028–1033, 2019, doi: 10.53555/jcr.v6:i7.13156.

[24] S. S. S. Neeli, “Critical Cybersecurity Strategies for Database Protection Against Cyber Attacks,” *J. Artif. Intell. Mach. Learn. Data Sci.*, vol. 1, no. 1, pp. 2102–2106, Nov. 2022, doi: 10.51219/JAIMLD/sethu-sesha-synam-neeli/461.

[25] B. Chaudhari and S. C. G. Verma, “Synergizing Generative AI and Machine Learning for Financial Credit Risk Forecasting and Code Auditing,” *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol.*, vol. 11, no. 2, pp. 2882–2893, Apr. 2025, doi: 10.32628/CSEIT25112761.

[26] T. Chen and C. Guestrin, “XGBoost: A scalable tree boosting system,” in *Proceedings of the ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, 2016. doi: 10.1145/2939672.2939785.

[27] T. Mokheleli and T. Museba, “Machine Learning Approach for Credit Score Predictions,” *J. Inf. Syst. Informatics*, vol. 5, no. 2, pp. 497–517, May 2023, doi: 10.51519/journalisi.v5i2.487.

[28] B. Oztas, D. Cetinkaya, F. Adedoyin, M. Budka, G. Aksu, and H. Dogan, “Transaction monitoring in anti-money laundering: A qualitative analysis and points of view from industry,” *Futur. Gener. Comput. Syst.*, vol. 159, pp. 161–171, Oct. 2024, doi: 10.1016/j.future.2024.05.027.

[29] H. O. Bello, C. Idemudia, and T. V. Iyelolu, “Integrating machine learning and blockchain: Conceptual frameworks for real-time fraud detection and prevention,” *World J. Adv. Res. Rev.*, vol. 23, no. 1, pp. 056–068, Jul. 2024, doi: 10.30574/wjarr.2024.23.1.1985.

[30] G. Maddali, “An Efficient Bio-Inspired Optimization Framework for Scalable Task Scheduling in Cloud Computing Environments,” *Int. J. Curr. Eng. Technol.*, vol. 15, no. 3, pp. 229–238, 2025.

[31] V. Prajapati, “Improving Fault Detection Accuracy in Semiconductor Manufacturing with Machine Learning Approaches,” *J. Glob. Res. Electron. Commun.*, vol. 1, no. 1, 2025.

[32] O. Olowu *et al.*, “AI-driven fraud detection in banking: A systematic review of data science approaches to enhancing cybersecurity,” *GSC Adv. Res. Rev.*, vol. 21, no. 2, pp. 227–237, Nov. 2024, doi: 10.30574/gscarr.2024.21.2.0418.

[33] W. Li, X. Liu, J. Su, and T. Cui, “Advancing financial risk management: A transparent framework for effective fraud detection,” *Financ. Res. Lett.*, vol. 75, p. 106865, Apr. 2025, doi: 10.1016/j.frl.2025.106865.

[34] B. Chaudhari and S. C. G. Verma, “Achieving High-Speed Data

Consistency in Financial Microservices Platforms Using NoSQL Using Nosql (Mongodb, Redis) Technologies," *Int. J. Adv. Res. Sci. Commun. Technol.*, pp. 750–759, Jun. 2024, doi: 10.48175/IJARSCT-18890.

[35] A. J. Samuel, A. J. Llc, and U. State, "Enhancing financial fraud detection with AI and cloud-based big data analytics : Security implications," *World J. Adv. Eng. Technol. Sci.*, vol. 09, no. 02, pp. 417–434, 2023.

[36] R. Q. Majumder, "A Review of Anomaly Identification in Finance Frauds Using Machine Learning Systems," *Int. J. Adv. Res. Sci. Commun. Technol.*, pp. 101–110, Apr. 2025, doi: 10.48175/IJARSCT-25619.

[37] B. Roshini, L. S. Gandham, P. S. Mandava, M. K. Enduri, and A. Tejaswi, "Enhanced Identification of Fraud in Credit Card Transactions Applying Machine Learning Strategies," in *2025 IEEE 14th International Conference on Communication Systems and Network Technologies (CSNT)*, 2025, pp. 148–152. doi: 10.1109/CSNT64827.2025.10967894.

[38] K. Hemanth, K. S. Virat, M. D. Rohith, K. V. P. Reddy, A. S. Selv, and S. P. S, "Credit Card Fraud Detection using Machine Learning Methods," in *2025 Emerging Technologies for Intelligent Systems (ETIS)*, 2025, pp. 1–6. doi: 10.1109/ETIS64005.2025.10961927.

[39] A. Kesharwani and P. Shukla, "FFDM − GNN:A Financial Fraud Detection Model using Graph Neural Network," in *2024 International Conference on Computing, Sciences and Communications (ICCSC)*, IEEE, Oct. 2024, pp. 1–6. doi: 10.1109/ICCSC62048.2024.10830438.

[40] M. Marripudugala, "AI-Powered Fraud Detection in the Financial Services Sector: A Machine Learning Approach," in *2024 2nd International Conference on Self Sustainable Artificial Intelligence Systems (ICSSAS)*, 2024, pp. 795–799. doi: 10.1109/ICSSAS64001.2024.10760599.

[41] M. Abbas, D. Almulla, A. Y. Alghasra, and M. Al-Shammari, "Applying Machine Learning to Detect Fraud of Financial Statements: A Systematic Literature Review," in *2024 International Conference on Decision Aid Sciences and Applications (DASA)*, IEEE, Dec. 2024, pp. 1–7. doi: 10.1109/DASA63652.2024.10836535.

[42] R. V. Jesus, D. A. Da Silva, J. A. S. Torres, F. L. L. De Mendonça, and R. T. De Sousa, "Open Source Intelligence: Classification and Mitigation of Risks and Fraud Within Financial Institutions," in *Iberian Conference on Information Systems and Technologies, CISTI*, 2023. doi: 10.23919/CISTI58278.2023.10211291.