IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 10, April 2025
Impact Factor: 7.67

A Review of Anomaly Identification in Finance Frauds Using Machine Learning Systems

Ruhul Quddus Majumder
Independent Researcher
Inforuhul@gmail.com

Abstract: *The growing prevalence of digital financial payments has caused fraud in financial services to significantly increase globally. Artificial learning-based abnormality to identifying anomalies must be used because traditional fraud detection methods are not very adaptable to contemporary dishonest methods. This review examines various machine learning methodologies, including deep learning, techniques for detecting fraud using autonomous, freestanding, and semi-supervised learning methods in banking, insurance, stock market processes, and digital payment transactions. The study highlights challenges associated with imbalanced data distributions and adversarial attacks, which impact detection performance and interpretability. Furthermore, the paper explores current developments in the integration of transparent artificial intelligence with graph-based anomaly identification technologies to improve fraud detection systems' transparency and credibility. The constraints of the investigation are evaluated in order to guide the creation of contemporary counterfeiting detection platforms that use several machine learning techniques for enhanced accuracy, real-time processing, and privacy preservation. The findings provide insights into designing robust fraud detection systems aligned with banking institutions' requirements, ensuring enhanced financial security and compliance.*

Keywords: Anomaly Detection, Financial Fraud, Machine Learning, Fraud Detection, Credit Card

I. INTRODUCTION

Financial statements serve as critical documents that encapsulate a company's financial performance, encompassing income, expenses, profits, loans, and managerial commentary. These statements, published quarterly and annually, provide transparency regarding business activities and allow stakeholders to evaluate the financial health and operational efficiency of an organization[1]. However, fraudulent manipulation of financial statements and transactions has emerged as a significant challenge, leading to substantial economic losses for governments, organizations, corporate entities, and individuals. Financial fraud undermines the integrity of financial institutions, eroding public trust and impacting the overall economy. It encompasses illicit activities that result in unauthorized financial gains through unethical or illegal means[2].

Anomaly detection contributes significantly to the detection of fraudulent activity by spotting anomalous patterns that diverge from typical transactional behavior. The identification of outliers and the detection of anomalies are frequently used indiscriminately, as they both focus on identifying deviations from expected behaviors. Various techniques have been developed for anomaly detection, leveraging data mining and ML methodologies to uncover fraudulent financial activities. These anomalies, also referred to as discordant objects, exceptions, aberrations, or contaminants, are indicative of potential fraudulent behavior.

To safeguard financial systems, organizations invest significantly in advanced technology and safety precautions to guard against attacks from the inside and the outside. Data-driven approaches, particularly those based on graph-based learning, have gained prominence in monitoring interactions and transactions within financial networks[3][4]. The relationships among entities in a network are analyzed by applying ML techniques to identify underlying irregularities that could signal fraudulent activities.

DOI: 10.48175/IJARSCT-25619

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 10, April 2025
Impact Factor: 7.67

Traditional fraud detection models typically operate on structured attribute-value datasets derived from transactional records. These models apply supervised and unsupervised learning techniques to classify transactions as fraudulent or legitimate[5][6]. However, challenges arise in detecting complex fraudulent behaviors such as money laundering, where transactions are inherently linked rather than independently distributed. The interdependencies in financial transactions necessitate advanced analytical models capable of handling linked data, which traditional methods often fail to address effectively.

The ML financial methods for identifying fraud have become widely used in a variety of fields, including stock exchange fraudulent activity, fraudulent use of credit cards, and other types of financial transaction anomalies. Recent studies have conducted comprehensive reviews on ML-driven fraud detection approaches, highlighting their effectiveness in mitigating fraudulent activities[7][8][9]. The evolution of ML-based techniques has significantly contributed to identifying and stopping financial fraud, providing a foundation for future research in this domain.

A.Structured of the paper

The paper is organized as following sections: Section II Methods for detecting anomalies in financial fraud Section III provide a ML approaches for financial fraud detection. Section IV Challenges, Limitations and future trends. Section V Literature Review, and Section VI concludes with future directions.

II. ANOMALY DETECTION TECHNIQUES IN FINANCIAL FRAUD

An anomaly identification technology for banking activities is called Deception Surveillance. Deception Guard learns how a user's financial transactions typically behave using ML. Transactions are marked as questionable if they diverge beyond this typical pattern[10]. Finding uncommon or abnormal data in a dataset is the primary goal of identifying anomalies and a crucial component of information mining. The ability to instinctively recognize intriguing and uncommon patterns in datasets makes recognizing anomalies fascinating. In statistical and ML, anomalous detection, also referred to as outlier identification, aberration being noticed, strangeness being noticed, and exception mining, has been extensively researched. When they may lead to crucial actions in a variety of pertinent areas, irregularities are relevant due to how they signal noteworthy but infrequent occurrences.

A. Anomaly Detection Techniques

The methods for supervised learning NN and DT are important yet uncommon occurrences that may lead to important decisions in a variety of different application areas. Identify fraud events with labeled data through extensive dataset requirements[11][12]. Self-Training and Variational Autoencoders as a technique enable semi-supervised learning systems to enhance their detection capability through the unification of small labeled data sets with unlimited unlabeled data. The anomaly detection approach in Unsupervised learning employs Isolation Forest and Autoencoders as tools for finding fraudulent patterns without requiring supervised tags. These detection procedures work best for identifying new fraudulent activities shown in Figure 1.

- **Supervised Anomaly:** The premise of supervised identification of anomalies approaches is that the data set being utilized is made up of annotated instances that belong to either the normal or anomalous class. The majority of methods in the latter group provide a prediction model for the normal and abnormal classes, which can then be used to classify newly discovered data. As was briefly mentioned before, a major problem with autonomous detecting anomalies is that the atypical class is often less common than the regular class[13].
- **Semi-supervised Anomaly:** Methods for semi-supervised recognition of anomalies make the assumption that the only annotated examples in the data set are those that fall into the standard class. They are thus more relevant. In contrast with unsupervised anomalies of anomalies, a framework is only built for the standard category and not the abnormal class. To find unusual occurrences, the test set of data is then contrasted with the model[14][15].
- **Unsupervised Anomaly:** Naturally all three groups, uncontrolled recognition without supervision is the most universally useful as the methods don't need any labels in the information set. In order to avoid larger instances

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 10, April 2025
Impact Factor: 7.67

of false alarms than anticipated, uncontrolled algorithms implicitly assume that abnormal occurrences are much less common than ordinary occurrences in the under scrutiny set of the information under consideration[16]. An unlabeled subsection of the training set of data is often used to apply semi-supervised techniques to an uncontrolled identification of anomaly issues.

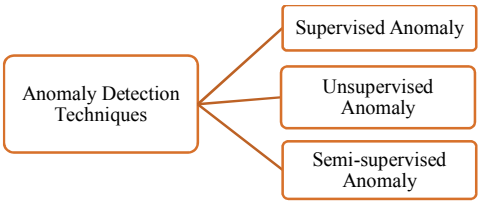

Figure 1: Anomaly Detection Techniques

B. Types of Anomalies

There are three types of abnormalities individual deviations, which are irregular data points contextual anomalies, which are normal in one context but aberrant in a different one; and aggregate anomalies, which are a collection of connected outliers indicating fraud). There are some of the anomaly types are explained below in Figure 2.

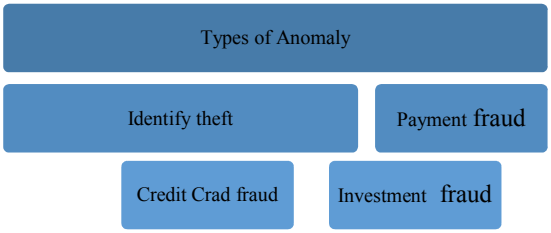

Figure 2: Types of Anomaly

- **Identity Theft:** The theft of identity is the unlawful acquisition and use of private data, such as banking account details or a social security number, with the goal of committing fraud. More complex methods of stealing someone's identity have also been made possible by developments in technology.
- **Payment Fraud:** The practices that target money transactions, such as credit card and cheque fraud, are included in fraud involving payments[17]. FIs should use diligence procedures while dealing with transactions and keep an eye out for anomalies in payment trends.
- **Credit Card Fraud:** The oldest and most prevalent form of fraud, as well as identity theft, is the fraudulent use of credit cards[16]. It is the unlawful use of a person's credit or debit card for creating transactions or taking out cash.
- **Investment Fraud:** The numerous strategies covered in this article are used in investment scams and frauds. Since fraudsters will go to considerable measures to make any web pages, papers, or information mentioned seem as authentic as achievable, many are going to be simpler to identify than others[18].

III. MACHINE LEARNING APPROACHES FOR FINANCIAL FRAUD DETECTION

There are numerous algorithms available for detecting fraud. However, because it all relies on what information you presently have, there isn't a single best ML technique for fraud detection[19][20].

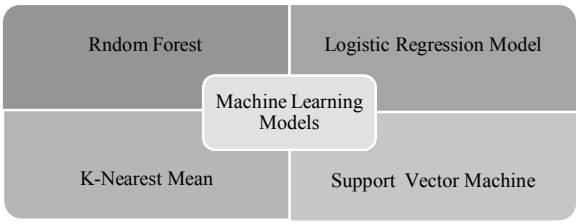

Figure 3: Machine learning models

DOI: 10.48175/IJARSCT-25619

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 10, April 2025
Impact Factor: 7.67

Figure 3 displays a list of some of the most well-known techniques; nevertheless, this is by no means an exhaustive list.

A. Logistic Regression (LR) Model

A popular statistical framework for applications involving classifications that are binary is LR[21]. It is a classification technique, not a regressive method, as the title suggests. It calculates the likelihood that a certain input is a member of a specified class. The LR model maps expected values to possibilities using the logistic function. The logistic function's outcome involves 0 and 1. LR divides inputs into two groups by establishing a threshold, often 0.5. using clinical data to determine whether a patient has a certain condition (such as diabetes or heart disease). Estimating the likelihood that a borrower would miss payments on a loan. using demographic and behavioral data to forecast a consumer's chances of making a buying decision

B. Support Vector Machines Model (SVM)

Support Vector Machines (SVM) was proposed to solve two-class classification problems[22]. The SVM deals with the principle of structural risk minimization to decrease its generalization error. It tries to find the optimum separating hyperplane (OSH) between two classes. The main goal is to maximize the margin between the classes of training samples. Support vector regression (SVR) is the promising extension of SVM to solve regression problems. This approach has shown successful results in many applications and various fields of study.

C. Decision Tree (DT) Model

The Testing and regression tasks benefit from the adaptable ML method known as decision trees. Each node in their decision structures represents a decision alongside its potential consequences that form a tree arrangement. The features in the model appear as nodes within the decision tree, while decision rules exist as connecting branches between nodes that lead to outcome leaves. The data splitting process at nodes depends on the feature which produces the most uniform subsets through an evaluation method (such as Gini impurity or information gain). Random forests comprise many decision trees that use the "bagging" approach for their training. The produced result of a random forest ensemble comes from averaging regression outputs and implementing majority voting for classification[23]. Forecasting the course of therapy and the outcomes for patients. Identification of fraud and risk control. Systems for client grouping and endorsement.

D. Random Forest Model

The introduction of ensemble decision-tree-based algorithms solved the overfitting issue of decision trees while random forest stands as a leading accurate and practical choice. Random forest classifiers construct several decision trees which merge their predictions through voting. Randomization emerges from both bagging and feature random sub-setting procedures. Through bootstrapping methods different data becomes available for tree creation while feature subset selection performs two-way randomization leading to consolidated weak learner models.

E. K-Nearest Mean (KNN) Model

A financial institution organized equivalent transactions using K-means clustering methods. Further evaluation occurred for all transactions that did not belong to any cluster grouping. This method uncovered new fraud patterns which enhanced the institution's fraud prevention capabilities during the process of identifying trading fraud activities[24]. Unsupervised anomaly detection methods identified transactions with abnormal behavior patterns through trading behavior analysis. The firm succeeded in uncovering insider trading infringements that routine inspection systems had overlooked. Detecting fraudulent insurance claims. The insurance organization used association rule learning to inspect their claims data through analysis. The analysis revealed unexpected patterns linking unconnected claims which thus made it possible to discover cooperative fraud activities

DOI: 10.48175/IJARSCT-25619

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 10, April 2025
Impact Factor: 7.67

There are some advantages of ML for fraud are explained below[25]:

- **Faster and efficient detection:** Machines are able to cut and paste enormous amounts of data given that they can process large datasets far more quickly than humans. That suggests More efficient and quick identifying objects The system is able to identify questionable trends and behaviors that individual employees would have missed for months[26].
- **Reduced manual review time:** The same to this you may drastically reduce the amount of time you spend going through material by having computers examine all of the evidence points for you.
- **Larger datasets improve predictions:** The greater amount of information you give an ML vehicle's engine, the more proficient it becomes. As a result, whereas huge amounts of data might often make it hard for humans to see patterns, an AI-driven system has exactly the opposite problem.
- **Cost-effective remedy:** Instead of integrating more Risks agents, you just need one machine-learning system to handle all the data that you throw at it, no matter how much of information you have. This is ideal for businesses who see seasonal variations in

IV. CHALLENGES, LIMITATIONS AND FUTURE DIRECTIONS IN FINANCIAL FRAUD DETECTION

Numerous advanced difficulties arise during the application of ML technology to detect financial fraud. The manifestation of fraud incidents remains lower than financial operations due to dataset imbalance which impedes model performance. The mechanisms used in fraud operations keep changing because criminals constantly advance their schemes to avoid detection protocols. Such adversarial attacks operate as an additional sixth method to modify ML models which enable attackers to escape identification systems. Multiple data types including transactions and user behaviors require refined integration methods because of their complex integration process. Synthetic data combines with obfuscation methods which fraudsters use to dodge detection systems among other forms of deception. False positive findings that break legal or ethical standards present a severe requirement since they generate financial losses for customers and lead to poor service satisfaction rates. The challenge is described below and also mentioned in Figure 4.

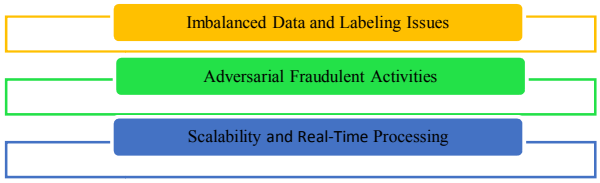

Figure 4: Challenges of Financial Fraud

A. Imbalanced Data and Labeling Issues

The latest data might change in a matter of minutes or even seconds. Thus, traditional categorization methods might not work effectively. Supervised education fails when the dataset has a large number of disparities in the geographical distribution of the data, as well as fluctuating information with high complexity and problem volume.

The growth of online transactions has skyrocketed in recent times and credit cards represent a significant portion of total online spending. An increasing number of people select credit cards to shop and execute e-commerce activities and educational transactions alongside e-wallet payments. Because banks and other involved stakeholders place high importance on fraud detection technology, they prioritize its development and maintenance. A wide range of fraudulent transactions exists. Online and Offline transactions represent their distribution. The research focuses on online transactions for explaining the ML solutions as an approach to managing them[27].

B. Adversarial Fraudulent Activities

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 10, April 2025
Impact Factor: 7.67

A static paradigm that serves as a filter for these fraudulent and legitimate activities is the standard paradigm for detecting fraud. However, reality depicts a very tense relationship between criminals and financial institutions, especially considering the high cost of credit card theft and the ease with which stolen credit card data can be retrieved from the dark web. In an effort to maximize stolen funds, fraudsters are always changing their tactics and trying to get past the fraud recognition algorithms. Credit card issuers' data scientists invest a lot of time and resources in thwarting fraudsters' attempts to learn the classifier and undermine its efficacy[28].

C. Scalability and Real-Time Processing

The analysis of data as it happens remains vital in finance sector applications because transaction surveillance requires instant data evaluation to track scams. The processing starts by collecting data which requires preprocessing. Different types of transaction data originate from point-of-sale mechanisms, online payments, mobile payment applications and bank wire transfers. The different sources deliver important results which enable the detection of financial fraud. Point-of-sale systems obtain retail transaction information simultaneously with online platform data collection for e-commerce recordings. Mobile payment systems enrich security by providing both user device information along with transaction location data to enrich authentication and detection capabilities for transaction data[29].

Future Trends in ML for Fraud Prevention

ML is developing quickly, with new developments in technology and trends influencing how prevention of fraud is done in the future. The subsequent sections emphasize important developments, such as the adoption of predictive as well as prescriptive analytics, the advancement of algorithms, the integration of other developing technology, and the growing emphasis on immediate data analysis. The following explains some possible paths in the future[30][31]:

- **Explainable AI (XAI):** Explore the complex areas of study and advancement related to Explainable AI (XAI). Deciphering the complexities of these approaches seeks to shed light on the opaque character of intricate models, opening the door for an explosion in openness that fosters confidence amongst law enforcement and investors alike.
- **Continuous Learning Models:** The creation of models starts as a dance with shifting fraud patterns. The system's real-time performance optimization occurs through dynamic online learning approaches orchestrated for continuous learning, which directs systems to serenely adjust when faced with fraud dynamics transformations.
- **Hybrid Models and Ensemble Approaches:** Explore the unexplored realms of model fusion using the alchemy of hybrid techniques and ensemble techniques. By combining the distinct brilliance of many models, an exquisite tapestry of fraud detection skill emerges, improving resistance and effectiveness.
- **Blockchain Technology:** The secretive understand sound of blockchain technology while exploring its implementation to make data security systems more resilient during financial transactions. Smart contracts deployed on blockchain platforms serve as a potential peak solution within digital soundscape that builds fraud-resistant financial security system[32].
- **Collaboration and Benchmarking:** Cultivate a cooperative environment between industry and educational institutions, planting the seeds for benchmarking measurements and datasets. The development of increasingly efficient fraud detection models is driven towards a harmonic conclusion by this musical standardization, which regulates fair assessments.

V. LITERATURE REVIEW

This section provides a comprehensive review of the literature on Anomaly Detection in Financial fraud using Machine Learning.

Haripriya et al. (2025) Ensuring security and identifying fraudulent activity have become critical concerns at a time when more and more financial transactions are being done online. Enhancing the effectiveness of current fraud detection systems necessitates the use of mostly higher order ML techniques. This paper investigates a hybrid strategy

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 10, April 2025
Impact Factor: 7.67

that combines anomaly detection based on autoencoders with XG Boost arrangement. By computing reconstruction losses, the autoencoder is used to detect departures from typical transaction patterns. The proposed model is implemented using Python software[33].

Inthavixay et al. (2024) aim to explore ways to protect the assets of customers and banks in Laos from falling victim to individuals with malicious intent who attempt to fraudulently steal customer assets online. New technologies, like anomaly detection models for financial transactions, safeguard customer and bank assets by filtering out suspicious activities before confirming the actual transaction. If the system detects an anomaly in a transaction, it will alert the account holder and ask for confirmation before proceeding with the transaction. they trained the anomaly detection model on a dataset of over 12 million records, utilizing techniques like IF, local outlier factor (LOF), and autoencoder (AE)[34].

Abbas et al. (2024) The primary objective of this study is to compile the body of current research, discover gaps in the field, and recommend future directions for research. Using the SLR approach, the research 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 machine learning's promise and capability to detect fraud in financial statements[35].

Hosseini et al. (2024) explore using uncontrolled ML techniques to identify unethical activity in the CEA market from 2018 to 2023. they evaluated several models, including Isolation Forest, One-Class SVM, Autoencoder, DBSCAN, LOF, K-Means, Elliptic Envelope, and PCA, using tick-by-tick trading data resampled into daily data. Volume outliers were identified using Z-scores, and their correlation with detected frauds was analyzed[36].

Kesharwani and Shukla (2024) introduce an innovative fraud detection model leveraging the power of Graph Neural Networks (GNN) to address these challenges. Their 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, their GNN model not only identifies anomalous patterns indicative of fraud but also adapts to evolving fraudulent tactics[37].

Geng and Zhang (2023) the losses due to credit card fraud exceed all measurable values for users who submit payments and the merchants who receive them, and the financial institutions who process transactions. Current anti-fraud techniques implement classification models consisting of CNN, LSTM and DNN. The traditional methods mainly employ original features during operations yet deliver inferior outcomes when facing unbalanced datasets. Contemporary models demand large amounts of annotated records for proper training procedures. The proposed study presents an unsupervised anomaly detection system based on dual adversarial learning, which detects credit card fraud[38].

Table I provides a structured swift of current studies on anomaly detection in financial fraud using ML. It highlights each study's focus area, key findings, challenges, and future research directions.

Table 1: Summary of Anomaly Detection in Financial Frauds Using Machine Learning approaches

Reference	Focus Area	Key Findings	Challenges	Future Work & Limitations
Haripriya et al. (2025)	Hybrid fraud detection using Autoencoder and XGBoost	Autoencoder computes reconstruction losses for anomaly detection; XGBoost classifies transactions	Need for higher-order ML algorithms; computational complexity	Further optimization of hybrid models; real-time fraud detection improvements
Inthavixay et al.(2024)	Anomaly detection in financial transactions using IF, LOF, AE	Trained on 12M+ records; alerts users before confirming transactions	False positives; latency in real-time detection	Enhancing model accuracy; real-world deployment at scale
Abbas et al. (2024)	Systematic Literature Review	Identifies effective ML algorithms; highlights	Lack of standardization;	Proposing a standardized

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 10, April 2025
Impact Factor: 7.67

	(SLR) on ML-based fraud detection	research gaps	varying dataset quality	framework for ML in fraud detection
Hosseini et al. (2024)	Unsupervised ML for fraud detection in CEA market	Used multiple unsupervised models; analyzed volume outliers with Z-scores	Difficulty in interpreting unsupervised results	Hybrid approaches combining supervised and unsupervised models
Kesharwani and Shukla, (2024)	Graph Neural Networks (GNN) for fraud detection	GNN captures complex relationships in financial transactions	Scalability & computational cost	Improving GNN adaptability to new fraud patterns
Geng and Zhang (2023)	Using competing learning methods to identify credit card fraud	presents a dual learning through competition unattended anomaly recognition network.	Performance on imbalanced datasets; requires large annotated datasets	Refining adversarial learning techniques; reducing dependency on labeled data

VI. CONCLUSION AND FUTURE WORK

The application of ML techniques enables financial institutions to successfully detect anomalous transactions for protecting themselves against risks through successful results. The three categories of ML methods including supervised learning and unsupervised learning together with graph-based learning prove useful for detecting financial fraudulent activities within different areas. Unbalanced dataset issues, changes in fraudulent techniques, and the need for interpretable models while managing data privacy concerns make it challenging to develop reliable fraud detection systems. While LR and DT, two common ML models, provide basic achievement, deep learning, when used in conjunction with GNNs performs better when applied to complicated patterns. fraud patterns. The continuous evolution of fraud detection strategies highlights the need for adaptive and scalable models to combat emerging threats in the financial sector.

Future studies should concentrate on improving the flexibility and efficiency of fraud detection systems by integrating real-time anomaly detection with explainable AI techniques. The use of hybrid models combining deep learning and traditional ML approaches can further improve detection accuracy. Additionally, addressing data privacy challenges through federated learning and blockchain-based fraud detection could enhance security while maintaining confidentiality. Moreover, the development of cost-sensitive models that minimize false positives without compromising fraud detection rates is crucial. Future studies should also explore automated feature engineering techniques and self-learning systems that can adapt to new fraud patterns with minimal human intervention. Lastly, cross-domain collaboration between financial institutions and regulatory bodies can help in building robust, industry-wide fraud detection frameworks.

REFERENCES

[1] M. N. Ashtiani and B. Raahemi, “Intelligent Fraud Detection in Financial Statements Using Machine Learning and Data Mining: A Systematic Literature Review,” 2022. doi: 10.1109/ACCESS.2021.3096799.

[2] K. G. Al-Hashedi and P. Magalingam, “Financial fraud detection applying data mining techniques: A comprehensive review from 2009 to 2019,” 2021. doi: 10.1016/j.cosrev.2021.100402.

[3] P. Chatterjee, “Smart Contracts and Machine Learning: Exploring Blockchain and AI in Fintech,” Indian J. Sci. Technol., vol. 18, no. 2, pp. 113–124, Jan. 2025, doi: 10.17485/IJST/v18i2.3838.

[4] T. Pourhabibi, K. L. Ong, B. H. Kam, and Y. L. Boo, “Fraud detection: A systematic literature review of graph-based anomaly detection approaches,” Decis. Support Syst., 2020, doi: 10.1016/j.dss.2020.113303.

[5] D. Huang, D. Mu, L. Yang, and X. Cai, “CoDetect: Financial Fraud Detection with Anomaly Feature Detection,” IEEE Access, 2018, doi: 10.1109/ACCESS.2018.2816564.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 10, April 2025 Impact Factor: 7.67

[6] D. D. Rao, A. A. Waoo, M. P. Singh, P. K. Pareek, S. Kamal, and S. V. Pandit, "Strategizing IoT Network Layer Security Through Advanced Intrusion Detection Systems and AI-Driven Threat Analysis," J. Intell. Syst. Internet Things, vol. 12, no. 2, pp. 195–207, 2024, doi: 10.54216/JISIoT.120215.
[7] A. Ali et al., "Financial Fraud Detection Based on Machine Learning: A Systematic Literature Review," 2022. doi: 10.3390/app12199637.
[8] S. S. S. Neeli, "Key Challenges and Strategies in Managing Databases for Data Science and Machine Learning," Int. J. Lead. Res. Publ., vol. 2, no. 3, p. 9, 2021.
[9] A. K. Aftab Arif, Muhammad Ismaeel Khan, "An overview of cyber threats generated by AI," Int. J. Multidiscip. Sci. Arts, vol. 3, no. 4, pp. 67–76, 2024.
[10] N. Bala, "Fraud Detection : Anomaly Detection System for Financial Transactions," vol. 8, no. 11, 2023.
[11] V. Pillai, "Anomaly Detection for Innovators: Transforming Data into Breakthroughs," Lib. Media Priv. Ltd., 2022.
[12] J. L. Deepak Dasaratha Rao, Sairam Madasu, Srinivasa Rao Gunturu, Ceres D'britto, "Cybersecurity Threat Detection Using Machine Learning in Cloud-Based Environments: A Comprehensive Study," Int. J. Recent Innov. Trends Comput. Commun., vol. 12, no. 1, 2024.
[13] N. Görnitz, M. Kloft, K. Rieck, and U. Brefeld, "Toward supervised anomaly detection," J. Artif. Intell. Res., 2013, doi: 10.1613/jair.3623.
[14] L. Ruff et al., "DEEP SEMI-SUPERVISED ANOMALY DETECTION," in 8th International Conference on Learning Representations, ICLR 2020, 2020.
[15] S. S. S. Neeli, "Critical Cybersecurity Strategies for Database Protection against Cyber Attacks," J. Artif. Intell. Mach. Learn. Data Sci., vol. 1, no. 1, p. 5, 2023.
[16] N. Malali, "AI Ethics in Financial Services : A Global Perspective," vol. 10, no. 2, 2025.
[17] B. K. R. Janumpally, "ARCHITECTING SERVERLESS PAYMENT GATEWAYS: A SYSTEMATIC ANALYSIS OF SCALE, SECURITY, AND PERFORMANCE TRADE-OFFS," IJRCAIT), vol. 8, no. 1, pp. 1186–1201, 2025.
[18] M. Shah, P. Shah, and S. Patil, "Secure and Efficient Fraud Detection Using Federated Learning and Distributed Search Databases," in 2025 IEEE 4th International Conference on AI in Cybersecurity (ICAIC), IEEE, Feb. 2025, pp. 1–6. doi: 10.1109/ICAIC63015.2025.10849280.
[19] V. Pillai, "System And Method For Intelligent Detection And Notification Of Anomalies In Financial And Insurance Data Using Machine Learning," Pat. Off. J., 2025.
[20] M. K. A Arif, A Khan, "Role of AI in Predicting and Mitigating Threats: A Comprehensive Review," JURIHUM J. Inov. dan Hum., vol. 2, no. 3, pp. 297–311, 2024.
[21] J. Kumar Chaudhary, S. Tyagi, H. Prapan Sharma, S. Vaseem 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 2023, 2023. doi: 10.1109/ICACITE57410.2023.10183344.
[22] M. Sabzekar and S. M. H. Hasheminejad, "Robust regression using support vector regressions," Chaos, Solitons & Fractals, vol. 144, p. 110738, 2021, doi: https://doi.org/10.1016/j.chaos.2021.110738.
[23] O. A. Bello, A. Folorunso, O. E. Ejiofor, F. Z. Budale, K. Adebayo, and O. A. Babatunde, "Machine Learning Approaches for Enhancing Fraud Prevention in Financial Transactions," Int. J. Manag. Technol., vol. 10, no. 1, pp. 85–108, 2023.
[24] M. Gopalsamy and K. B. Dastageer, "The Role of Ethical Hacking and AI in Proactive Cyber Defense : Current Approaches and Future Perspectives," vol. 10, no. 2, 2025.
[25] Sumukh Uday Rabade, "Use of Machine Learning in Financial Fraud Detection: A Review," Int. J. Adv. Res. Sci. Commun. Technol., 2022, doi: 10.48175/ijarsct-7595.
[26] S. Radadia, K. Dodiya, and K. Shukla, "Innovative Cyber Security Detecting and Alerting Device: An Integrated Approach to Threat Detection and Mitigation," Int. Res. J. Eng. Technol., vol. 11, no. 8, 2024.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 10, April 2025
Impact Factor: 7.67

[27] "Analysis of Credit Card Fraud detection using Machine Learning models on balanced and imbalanced datasets," Int. J. Emerg. Trends Eng. Res., 2021, doi: 10.30534/ijeter/2021/02972021.
[28] A. Mead, T. Lewris, S. Prasanth, S. Adams, P. Alonzi, and P. Beling, "Detecting fraud in adversarial environments: A reinforcement learning approach," in 2018 Systems and Information Engineering Design Symposium, SIEDS 2018, 2018. doi: 10.1109/SIEDS.2018.8374720.
[29] Halima Oluwabunmi Bello, Adebimpe Bolatito Ige, and Maxwell Nana Ameyaw, "Adaptive machine learning models: Concepts for real-time financial fraud prevention in dynamic environments," World J. Adv. Eng. Technol. Sci., vol. 12, no. 2, pp. 021–034, Jul. 2024, doi: 10.30574/wjaets.2024.12.2.0266.
[30] P. Kamuangu, "A Review on Financial Fraud Detection using AI and Machine Learning," J. Econ. Financ. Account. Stud., 2024, doi: 10.32996/jefas.2024.6.1.7.
[31] S. Tyagi, T. Jindal, S. H. Krishna, S. M. Hassen, S. K. Shukla, and C. Kaur, "Comparative Analysis of Artificial Intelligence and its Powered Technologies Applications in the Finance Sector," in Proceedings of 5th International Conference on Contemporary Computing and Informatics, IC3I 2022, 2022. doi: 10.1109/IC3I56241.2022.10073077.
[32] Suhag Pandya, "Innovative blockchain solutions for enhanced security and verifiability of academic credentials," Int. J. Sci. Res. Arch., vol. 6, no. 1, pp. 347–357, Jun. 2022, doi: 10.30574/ijsra.2022.6.1.0225.
[33] T. Haripriya, S. Chandramouli, M. Kavitha, M. D. Parne, D. Srinivas, and B. K. Bala, "Machine Learning Algorithms for Dynamic Financial Management and Fraud Detection: Implementing Anomaly Detection, and Risk Assessment Techniques," in 2025 International Conference on Intelligent Systems and Computational Networks (ICISCN), 2025, pp. 1–6. doi: 10.1109/ICISCN64258.2025.10934386.
[34] S. Inthavixay, S. Inthasone, A. Chanthaphavong, and T. Keophilavong, "Utilizing Machine Learning Techniques to Identify Anomalies in Financial Transactions for Laos Banking," in 2024 7th International Conference on Information and Communications Technology (ICOIACT), 2024, pp. 79–84. doi: 10.1109/ICOIACT64819.2024.10913217.
[35] 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.
[36] S. A. Hosseini, F. Grimaccia, A. Niccolai, M. Lorenzo, and F. Casamatta, "Potential Fraud Detection in Carbon Emission Allowance Markets Using Unsupervised Machine Learning Models," in 2024 10th International Conference on Signal Processing and Intelligent Systems (ICSPIS), IEEE, Dec. 2024, pp. 33–37. doi: 10.1109/ICSPIS65223.2024.10931097.
[37] 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.
[38] J. Geng and B. Zhang, "Credit Card Fraud Detection Using Adversarial Learning," in 2023 International Conference on Image Processing, Computer Vision and Machine Learning, ICICML 2023, 2023. doi: 10.1109/ICICML60161.2023.10424872.