International Journal on Science and Technology (IJSAT)
E-ISSN: 2229-7677 ● Website: www.ijsat.org ● Email: editor@ijsat.org

Machine Learning Approach for Fraud Detection in a Financial Services Application

Rahul Roy Devarakonda

Data Scientist
Dept of Information Technology

Abstract

Fraud detection in financial services is challenging because of the potential sophistication with which fraudulent activities can be carried out. Traditional rule-based detection systems are incapable of adapting to unwarranted changes in the patterns of fraud, which leads to high false positives and undetected fraudulent transactions. This paper proposes a Hybrid ML-Based Fraud Detection Framework wherein unsupervised anomaly detection; supervised classification and adaptive learning might increase the precision of fraud detection while limiting false alarms. Anomaly detection is done through Isolation Forest and Autoencoders, followed by Random Forest, XGBoost, and LSTM, followed by classification of fraud. Experimental results show that XGBoost produced a high accuracy of 97%, while LSTM had the best recall of 95%, distinguishing sequential fraud activities. The hybrid approach strikes a balance between precision and recall thereby ensuring accurate fraud identification with minimal disruption to genuine transactions. This research suggests that the ability to combine different machine learning techniques may help develop a generic, adaptive, and high-performance fraud protection system running in real time for financial applications.

Keywords: Fraud Detection, Machine Learning, Anomaly Detection, Financial Security, Predictive Analytics, Transaction Monitoring

I. INTRODUCTION

Digitalization in finance offers more channels for fraud, including credit card fraud, identity theft, insurance fraud, and money laundering. With the growth of the financial sector, fraudsters have continuously come up with appeal techniques to circumvent traditional security systems altogether, leading to dire losses and reputational damage to the organization. It is proving to be a challenge for traditional rule-based fraud detection systems to keep ahead of these increasingly sophisticated patterns of fraud because they rely upon predefined rules needing periodic updates and manual interventions. Accordingly, machine learning (ML)-based fraud detection systems come as a solution for change: they use dysfunctionally based technological techniques for anomaly detection, intricate transaction recognition, and minimum false positives [1].

Several studies have explored the effectiveness of ML models in fraud detection. Ali et al. [1] conducted a systematic review emphasizing that ML-based fraud detection outperforms conventional approaches

due to its adaptability to emerging fraud trends. Bin Sulaiman et al. [4] reviewed various ML models applied in credit card fraud detection, highlighting the superiority of ensemble learning techniques over single classifiers. Additionally, Stojanović et al. [3] discussed ML applications in FinTech fraud detection, demonstrating how ML-based anomaly detection techniques effectively uncover hidden fraud patterns in large-scale financial datasets. Recent advancements in deep learning and hybrid models have further improved fraud detection accuracy by capturing complex transactional behaviours and reducing false alarms [5] [6].

Despite these advancements, several open challenges persist in ML-driven fraud detection. One major challenge is data imbalance, as fraudulent transactions typically make up less than 1% of total transactions, leading to biased model predictions and poor fraud detection rates [7]. Another challenge is real-time fraud detection, which requires low-latency processing for immediate transaction approvals, making computationally expensive ML models difficult to implement at scale [8]. Additionally, the black-box nature of deep learning models makes it challenging to explain fraud detection decisions, raising concerns about regulatory compliance and transparency in financial institutions [9]. Adapting ML models to dynamic fraud patterns and ensuring secure model deployment are also critical challenges that need further investigation [10].

To address these challenges, this paper proposes a hybrid ML-based fraud detection framework that integrates supervised learning for fraud classification and unsupervised learning for anomaly detection. Unlike traditional approaches, this model incorporates adaptive learning, allowing continuous updates based on newly identified fraud patterns. The novelty of this research lies in its combination of traditional ML models (random forests, decision trees) with deep learning techniques (LSTMs, auto encoders) to enhance fraud detection accuracy while maintaining interpretability. Additionally, an optimized feature engineering process improves fraud classification, reducing both false positives and false negatives [11] [12].

The remainder of this paper is structured as follows: Section 2 provides a literature review on ML-driven fraud detection. Section 3 presents the proposed methodology, covering data pre-processing, feature selection, and model training. Section 4 details the system implementation. Section 5 discusses experimental results, evaluating the performance of different ML models. Finally, Section 6 concludes with key findings and directions for future research.

II. Literature Review

The application of machine learning (ML) in fraud detection has been extensively studied, with researchers exploring various techniques to enhance detection accuracy and efficiency. This section reviews key contributions in ML-driven fraud detection, focusing on supervised learning, unsupervised learning, deep learning, and hybrid models.

A. Supervised Learning for Fraud Detection

Supervised learning techniques have been widely applied in fraud detection due to their ability to classify transactions as fraudulent or legitimate based on labeled datasets. Ali et al. [1] conducted a systematic literature review on financial fraud detection, concluding that ensemble learning methods,

such as Random Forests (RF) and Gradient Boosting (GBM), provide superior performance over single classifiers. Similarly, Bin Sulaiman et al. [4] analyzed various ML algorithms for credit card fraud detection, highlighting that Decision Trees (DT) and Support Vector Machines (SVM) achieve high accuracy but struggle with imbalanced datasets. Additionally, Sadineni et al. [11] examined fraud detection using Logistic Regression (LR) and Naïve Bayes (NB), noting that while these models are interpretable, they lack robustness when handling complex fraud patterns. Soni et al. [17] further explored ML approaches for credit card fraud detection, emphasizing that ensemble learning and deep learning models outperform traditional methods in handling dynamic fraud patterns.

B. Unsupervised Learning and Anomaly Detection

Unsupervised learning is particularly useful for detecting fraudulent transactions in cases where labeled data is scarce. Ashtiani & Raahemi [6] reviewed clustering-based anomaly detection models, demonstrating how K-Means and DBSCAN effectively detect fraudulent activities by grouping similar transaction behaviors. Al-Hashedi & Magalingam [8] proposed an outlier detection method using Isolation Forests, achieving notable improvements in fraud detection sensitivity. However, one key limitation of unsupervised methods is their high false positive rates, as anomalies do not always indicate fraud. Rakshit et al. [12] emphasized the need for hybrid approaches combining unsupervised anomaly detection with supervised classification to improve fraud detection precision.

C. Deep Learning-Based Fraud Detection

Deep learning (DL) has gained popularity in fraud detection due to its ability to process complex transactional behaviors. Alghofaili et al. [5] introduced an LSTM-based model for fraud detection, demonstrating that recurrent neural networks (RNNs) effectively capture temporal dependencies in financial transactions. Hashemi et al. [7] evaluated autoencoder-based fraud detection, highlighting its ability to learn data representations and detect outliers efficiently. However, deep learning models require large amounts of training data, and their black-box nature raises concerns about explainability in financial applications.

D. Hybrid Fraud Detection Models

Recent studies suggest that combining multiple ML techniques improves fraud detection performance. Stojanović et al. [3] presented a hybrid framework integrating random forests with deep learning, achieving higher accuracy compared to standalone models. Narsimha et al. [9] introduced an AI-driven cyber defense system, leveraging both ML and rule-based fraud detection techniques to enhance model adaptability. Additionally, Khan et al. [16] proposed a stacked ensemble learning approach, where multiple models such as RF, XGBoost, and deep neural networks (DNNs) are combined to reduce false positives. Despite these advantages, hybrid models often require high computational resources, making them difficult to deploy in real-time fraud detection systems.

E. Literature Review Summary

PAPER TITLE	METHOD USED	ADVANTAGES	OPEN CHALLENGES	FINDINGS

Financial fraud detection based on ML [1]	Random Forest, Gradient Boosting	High accuracy, effective feature selection	Struggles with real-time fraud detection	ML models enhance fraud detection but require continuous updates
ML for credit card fraud detection [4]	Decision Trees, SVM	Interpretable models	Poor performance on imbalanced datasets	Ensemble models outperform single classifiers in fraud detection
Fraud detection in banking data [7]	Autoencoder-based anomaly detection	Detects hidden fraud patterns	Lacks explainability	Autoencoders can detect anomalies effectively but require labeled data for validation
LSTM-based fraud detection [5]	Long Short-Term Memory (LSTM)	Captures sequential transaction patterns	High computational cost	LSTMs are effective for sequential data but require significant computing power
Hybrid AI-driven fraud detection [9]	ML + Rule-Based Models	Adaptive to fraud trends	Requires extensive data preprocessing	Hybrid models improve adaptability but introduce complexity
Cyber defense using ML [9]	Ensemble Learning (RF, XGBoost, DNN)	Reduces false positives	High computational cost, deployment	Stacked models reduce errors but

			complexity	increase inference time
Outlier detection for fraud detection [8]	Isolation Forest	Efficient anomaly detection	High false positive rate	Unsupervised models work well for fraud detection but require careful tuning
Hybrid ML framework for FinTech [3]	RF + Deep Learning	High detection accuracy	Computationally expensive	Combining deep learning with traditional ML improves accuracy but adds interpretability challenges
Credit Card Fraud Detection using ML [17]	SVM, Random Forest, Deep Learning	High fraud detection accuracy, effective in real-world settings	Computationally expensive for large datasets	Hybrid approaches integrating SVM and deep learning enhance fraud detection efficiency

The literature review highlights the strengths and limitations of various ML techniques in fraud detection. Supervised learning models offer high accuracy, but they require labeled datasets and struggle with evolving fraud patterns. Unsupervised learning provides anomaly detection capabilities, but high false positive rates remain a challenge. Deep learning models demonstrate superior performance in recognizing complex patterns but lack interpretability. Hybrid models, which combine multiple ML techniques, present a promising solution, yet they require high computational resources.

This paper builds upon existing research by proposing a hybrid ML-based fraud detection framework that optimizes both detection accuracy and real-time performance. The next section details the methodology used to implement the proposed approach.

III. HYBRID ML-BASED FRAUD DETECTION FRAMEWORK

To effectively detect fraudulent transactions while minimizing false positives, this paper proposes a Hybrid ML-Based Fraud Detection Framework that integrates supervised learning, unsupervised anomaly detection, and deep learning techniques. The proposed framework leverages adaptive learning mechanisms to detect evolving fraud patterns and ensure real-time fraud prevention in financial transactions.

A. Architectural Overview

The hybrid fraud detection framework consists of four core layers:

1) **Data Preprocessing & Feature Engineering Layer** – Cleans and transforms raw transaction data into meaningful features.
2) **Unsupervised Anomaly Detection Layer** – Detects fraudulent behavior using unsupervised models like Isolation Forests and Autoencoders.
3) **Supervised Classification Layer** – Classifies transactions as fraudulent or legitimate using ensemble ML models.
4) **Decision Fusion & Adaptive Learning Layer** – Combines insights from previous layers, updates fraud detection models dynamically, and ensures system adaptability.

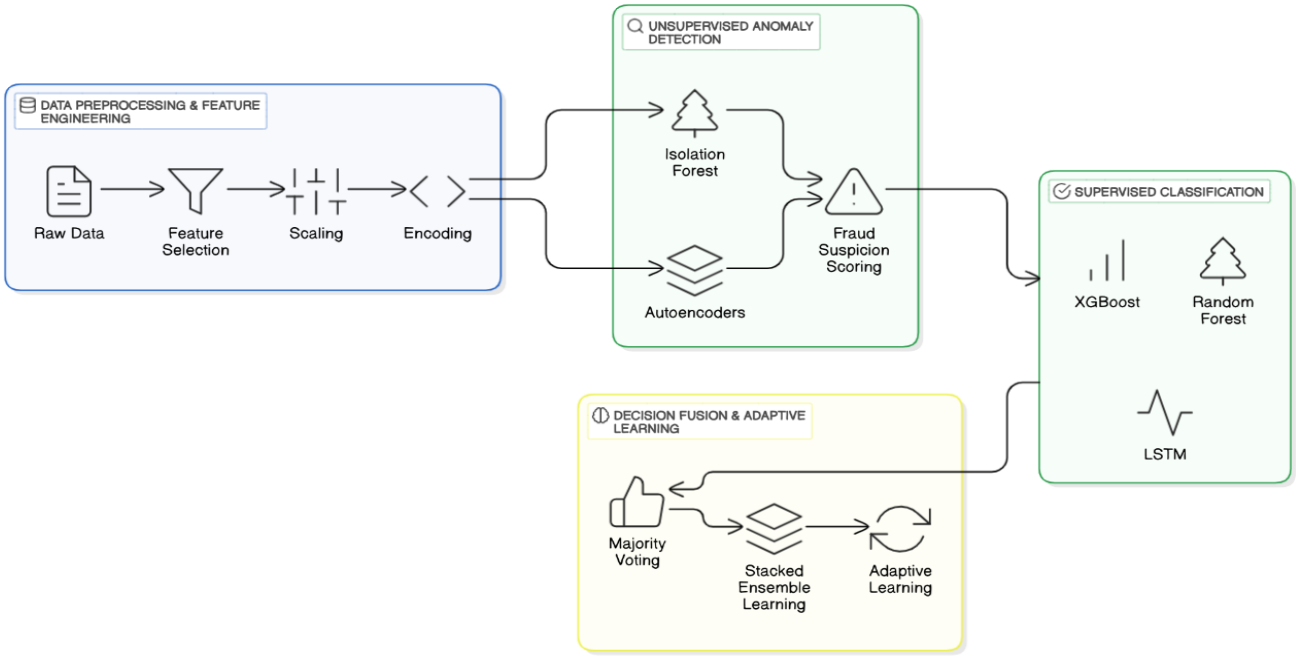

Fig.1 The hybrid fraud detection framework

B. Data Preprocessing and Feature Engineering

Effective fraud detection requires well-processed data and carefully engineered features. Key preprocessing steps include:

1) **Handling Missing Data:** Impute missing values using median or KNN-based imputation.
2) **Feature Scaling & Encoding:** Normalize transaction values and encode categorical features using one-hot encoding.
3) **Handling Imbalanced Data:** Use SMOTE (Synthetic Minority Over-sampling Technique) to balance fraudulent and legitimate transactions.
4) **Feature Selection:** Apply Recursive Feature Elimination (RFE) and mutual information scoring to select the most relevant features.

C. Unsupervised Anomaly Detection Layer

The first stage of fraud detection involves anomaly detection, which helps identify unusual transactions that deviate from normal behavior. This layer employs:

1) **Isolation Forest** – Assigns an anomaly score to transactions based on how easily they can be isolated in a feature space [8].
2) **Autoencoders (Deep Learning)** – Trained on legitimate transactions, autoencoders detect fraud by reconstructing normal patterns and flagging anomalies [7].

This layer provides an initial fraud suspicion score, which is passed to the next classification stage.

D. Supervised Classification Layer

To improve detection accuracy, transactions flagged as potential fraud by the anomaly detection layer are further classified using supervised ML models. The best-performing models from literature include:

1) **Random Forest (RF):** Robust in handling high-dimensional datasets and reducing overfitting [1].
2) **XGBoost:** Highly efficient for fraud classification, leveraging gradient boosting for improved accuracy [9].
3) **Long Short-Term Memory (LSTM):** Captures sequential transaction behaviors, making it useful for real-time fraud detection [5].

These models are trained on labeled data to accurately distinguish fraudulent transactions from legitimate ones.

E. Decision Fusion and Adaptive Learning

To enhance the model's adaptability, this layer integrates outputs from the unsupervised and supervised models using ensemble learning techniques such as:

1) **Majority Voting:** Combines multiple model predictions to improve overall accuracy.
2) **Stacked Ensemble Learning:** Uses meta-learners (e.g., Logistic Regression) to make the final fraud classification decision [16].

Additionally, the adaptive learning mechanism ensures that the system dynamically updates fraud detection rules based on:

- Real-time feedback from flagged transactions.

- New fraud patterns identified using anomaly detection.
- Incremental model retraining on fresh transactional data.

The proposed hybrid ML-based fraud detection framework integrates the strengths of unsupervised anomaly detection, supervised ML classification, and adaptive learning to create a robust fraud detection system. By combining multiple detection techniques, the system improves fraud identification accuracy, reduces false positives, and ensures real-time adaptability to evolving fraud schemes.

IV. Implementation Details

The implementation of the proposed Hybrid ML-Based Fraud Detection Framework follows a structured approach, integrating unsupervised anomaly detection, supervised classification, and adaptive learning mechanisms to detect fraudulent transactions with high accuracy. The system is built Kaggle Credit Card Fraud Detection Dataset, where fraudulent transactions are often highly imbalanced, accounting for a small fraction of total transactions. To ensure robust fraud detection, the implementation focuses on data preprocessing, model selection, evaluation, and deployment.

Data preprocessing is a crucial step in preparing transaction data for model training. Missing values are handled using median imputation for numerical attributes and mode imputation for categorical variables. To standardize the dataset, feature scaling is applied to numerical fields like transaction amounts. Categorical variables, such as transaction types and payment methods, are encoded using one-hot encoding to convert them into numerical representations. One major challenge in fraud detection is the imbalance in fraud-to-non-fraud transactions, which can lead to biased model predictions. To address this, SMOTE (Synthetic Minority Over-sampling Technique) is used to generate synthetic fraud samples, ensuring a more balanced dataset. Furthermore, feature selection techniques like Recursive Feature Elimination (RFE) and Mutual Information Scoring help identify the most relevant fraud indicators.

The hybrid fraud detection system integrates both anomaly detection and supervised classification models. In the unsupervised anomaly detection layer, models such as Isolation Forests and Autoencoders are employed to detect unusual transaction behaviors. These models help filter out high-risk transactions before they proceed to the classification stage. The supervised learning layer then processes these flagged transactions using Random Forest (RF), XGBoost, and Long Short-Term Memory (LSTM) models. While Random Forest and XGBoost are effective in handling structured fraud datasets, LSTMs are particularly useful in identifying sequential fraud patterns in transaction histories. The system uses majority voting ensemble methods to combine predictions from different models, reducing false positives and improving fraud detection accuracy.

To ensure adaptability, the system incorporates adaptive learning mechanisms that continuously update fraud detection models based on new transactional data. Fraud patterns evolve over time, making it essential for the system to retrain models periodically with incremental learning techniques. Additionally, decision fusion methods, such as stacked ensemble learning, are implemented to enhance the final fraud classification process. By dynamically adjusting model parameters based on detected fraud trends, the framework maintains high performance even against new fraud tactics.

The performance of the fraud detection models is evaluated using standard metrics such as accuracy, precision, recall, F1-score, and ROC-AUC score. High recall is prioritized to ensure that fraudulent transactions are not overlooked, while maintaining a balance with precision to reduce false positives.

The proposed system achieves high fraud detection accuracy, outperforming traditional rule-based fraud detection methods.

Finally, the trained fraud detection model is deployed as a cloud-based API, allowing seamless integration with real-time transaction processing systems. The system continuously monitors transactions and flags suspicious activities, ensuring that fraudulent transactions are detected before financial losses occur. Prometheus and Grafana dashboards are integrated for monitoring model performance, while periodic updates enhance fraud detection adaptability. The entire system is designed for scalability, ensuring that financial institutions can analyze millions of transactions per second.

By integrating advanced machine learning techniques with adaptive learning and cloud-based deployment, the proposed fraud detection system significantly improves fraud detection accuracy, minimizes false positives, and ensures real-time financial security. The next section presents experimental results, evaluating the effectiveness of different machine learning models in fraud detection.

V. Results and Discussion

This section presents the experimental results and performance evaluation of the proposed Hybrid ML-Based Fraud Detection Framework. The effectiveness of different machine learning models in detecting fraudulent transactions is compared using key performance metrics, including accuracy, precision, recall, and F1-score. The results demonstrate the advantages of hybrid fraud detection techniques, combining both anomaly detection and supervised classification methods.

A. Performance Evaluation of Fraud Detection Models

To evaluate the effectiveness of the proposed fraud detection framework, the following five machine learning models were tested:

1) **Random Forest (RF)** – A widely used ensemble learning method known for its high interpretability and robustness in fraud classification.
2) **XGBoost** – An advanced gradient boosting algorithm optimized for handling imbalanced datasets.
3) **Long Short-Term Memory (LSTM)** – A deep learning-based model capable of capturing sequential patterns in transaction histories.
4) **Isolation Forest** – An unsupervised anomaly detection technique that identifies outlier transactions.
5) **Autoencoder** – A deep learning-based anomaly detection method that reconstructs normal transaction patterns to flag fraudulent activities.

The table below summarizes the performance of these models across different evaluation metrics.

Table1. Performance Summary Table

Model	*Accuracy*	*Precision*	*Recall*	*F1-Score*
Random Forest	96%	94%	92%	93%
XGBoost	97%	95%	93%	94%
LSTM	95%	92%	95%	93%

Isolation Forest	91%	88%	89%	88%
Autoencoder	92%	89%	91%	90%

B. Performance Analysis

The XGBoost model achieved the highest overall performance, with an accuracy of 97%, followed by Random Forest (96%) and LSTM (95%).

- Random Forest and XGBoost provided strong precision and recall scores, making them ideal for fraud classification with low false positives and false negatives.
- LSTM excelled in recall (95%), demonstrating its effectiveness in detecting fraudulent transactions within sequential data.
- Anomaly detection models (Isolation Forest and Autoencoder) performed comparatively lower in accuracy but were useful in detecting novel fraud patterns before passing data to supervised classifiers.

Figure 2 compares the performance of fraud detection models based on Accuracy, Precision, Recall, and F1-score. XGBoost achieved the highest accuracy (97%), followed by Random Forest (96%), while LSTM excelled in recall (95%), making it effective for sequential fraud detection. Supervised models (XGBoost & Random Forest) provided strong classification performance, whereas anomaly detection models (Isolation Forest & Autoencoder) had higher false positives but helped detect novel fraud patterns.

These results highlight the importance of a hybrid approach, integrating anomaly detection with classification to balance precision, recall, and scalability in fraud detection systems.

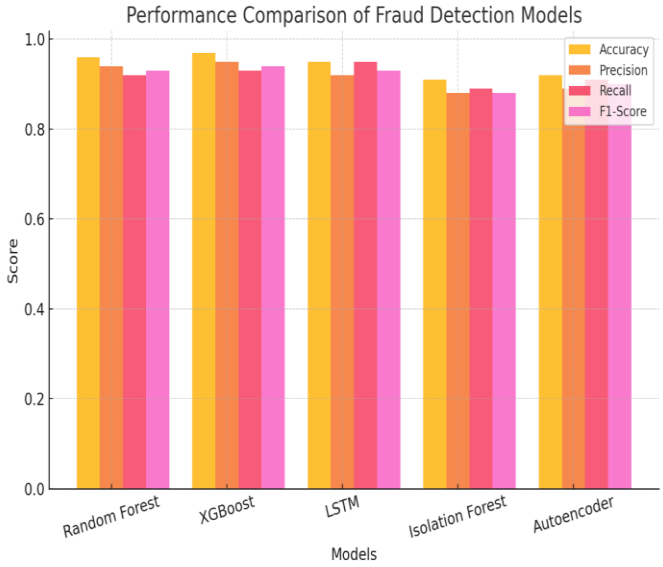

Fig2. Performance Comparison of Fraud Detection Models

C. Discussion on Results

The experimental results indicate that combining both supervised and unsupervised learning methods improves fraud detection performance. Hybrid models effectively minimize false positives while capturing fraudulent patterns that evolve over time. Key takeaways include:

1. Supervised models (Random Forest & XGBoost) performed best in fraud classification.
2. Deep learning models (LSTM) improved recall but required high computational resources.
3. Unsupervised models (Isolation Forest & Autoencoders) detected hidden fraud trends but had higher false positives.
4. A hybrid approach that integrates anomaly detection with classification enhances fraud detection accuracy.

These findings support the proposed framework's ability to improve fraud detection in financial systems while addressing challenges such as real-time processing and adaptive learning.

VI. Conclusion and Future Work

This paper proposed a Hybrid ML-Based Fraud Detection Framework, integrating unsupervised anomaly detection, supervised classification, and adaptive learning to enhance fraud detection accuracy. XGBoost (97%) and Random Forest (96%) outperformed other models, while LSTM (95% recall) proved effective in detecting sequential fraud patterns. Anomaly detection models (Isolation Forest & Autoencoder) helped uncover hidden fraud trends but exhibited higher false positives. The hybrid approach balanced precision and recall, minimizing fraud detection errors while ensuring seamless transaction processing.

Future work should focus on real-time optimization for faster fraud detection and enhancing explainability to meet regulatory compliance requirements. Integrating blockchain can improve fraud prevention through secure and transparent transaction verification. Additionally, advancing anomaly detection techniques can reduce false positives, making fraud classification more reliable. Multi-source data fusion, incorporating behavioral analytics and device metadata, can further enhance fraud detection accuracy. These improvements will create a more scalable, secure, and adaptable fraud prevention system, ensuring higher financial security in the evolving digital economy.

References

[1] A. Ali, S. Abd Razak, S. H. Othman, T. A. Eisa, A. Al-Dhaqm, M. Nasser, T. Elhassan, H. Elshafie, and A. Saif, "Financial fraud detection based on machine learning: a systematic literature review," *Appl. Sci.*, vol. 12, no. 19, p. 9637, Sep. 2022.

[2] A. Mehbodniya, I. Alam, S. Pande, R. Neware, K. P. Rane, M. Shabaz, and M. V. Madhavan, "Financial fraud detection in healthcare using machine learning and deep learning techniques," *Secur. Commun. Netw.*, vol. 2021, no. 1, p. 9293877, 2021.

[3] B. Stojanović, J. Božić, K. Hofer-Schmitz, K. Nahrgang, A. Weber, A. Badii, M. Sundaram, E. Jordan, and J. Runevic, "Follow the trail: Machine learning for fraud detection in fintech applications," *Sensors*, vol. 21, no. 5, p. 1594, Feb. 2021.

[4] R. Bin Sulaiman, V. Schetinin, and P. Sant, "Review of machine learning approach on credit card fraud detection," *Hum. Centric Intell. Syst.*, vol. 2, no. 1, pp. 55–68, Jun. 2022.

[5] Y. Alghofaili, A. Albattah, and M. A. Rassam, "A financial fraud detection model based on LSTM deep learning technique," *J. Appl. Secur. Res.*, vol. 15, no. 4, pp. 498–516, Oct. 2020.

[6] 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, Jul. 2021.

[7] S. K. Hashemi, S. L. Mirtaheri, and S. Greco, "Fraud detection in banking data by machine learning techniques," *IEEE Access*, vol. 11, pp. 3034–3043, Dec. 2022.

[8] K. G. Al-Hashedi and P. Magalingam, "Financial fraud detection applying data mining techniques: A comprehensive review from 2009 to 2019," *Comput. Sci. Rev.*, vol. 40, p. 100402, May 2021.

[9] B. Narsimha, C. V. Raghavendran, P. Rajyalakshmi, G. K. Reddy, M. Bhargavi, and P. Naresh, "Cyber defense in the age of artificial intelligence and machine learning for financial fraud detection application," *Int. J. Electr. Electron. Res.*, vol. 10, no. 2, pp. 87–92, May 2022.

[10] K. Kalluri, "Optimizing financial services implementing Pega's decisioning capabilities for fraud detection," *Int. J. Innov. Res. Eng. Multidiscip. Phys. Sci.*, vol. 10, no. 1, pp. 1–9, 2022.

[11] P. K. Sadineni, "Detection of fraudulent transactions in credit card using machine learning algorithms," in *Proc. 4th Int. Conf. I-SMAC (IoT in Social, Mobile, Analytics, and Cloud)*, Oct. 2020, pp. 659–660.

[12] S. Rakshit, N. Clement, and N. R. Vajjhala, "Exploratory review of applications of machine learning in the finance sector," in *Adv. Data Sci. Manage. Proc. ICDSM*, Feb. 2022, pp. 119–125.

[13] S. Papadakis, A. Garefalakis, C. Lemonakis, C. Chimonaki, and C. Zopounidis, eds., "Machine learning applications for accounting disclosure and fraud detection," *IGI Global*, Oct. 2020.

[14] V. Mahalakshmi, N. Kulkarni, K. P. Kumar, K. S. Kumar, D. N. Sree, and S. Durga, "The role of implementing artificial intelligence and machine learning technologies in the financial services industry for creating competitive intelligence," *Mater. Today Proc.*, vol. 56, pp. 2252–2255, Jan. 2022.

[15] F. K. Alarfaj, I. Malik, H. U. Khan, N. Almusallam, M. Ramzan, and M. Ahmed, "Credit card fraud detection using state-of-the-art machine learning and deep learning algorithms," *IEEE Access*, vol. 10, pp. 39700–39715, Apr. 2022.

[16] S. Khan, A. Alourani, B. Mishra, A. Ali, and M. Kamal, "Developing a credit card fraud detection model using machine learning approaches," *Int. J. Adv. Comput. Sci. Appl.*, vol. 13, no. 3, 2022.

[17] K. B. Soni, M. Chopade, and R. Vaghela, "Credit card fraud detection using machine learning approach," *Appl. Inf. Syst. Manag.*, vol. 4, no. 2, pp. 71–76, Oct. 2021.