Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 03, March-2025

An Overview of Deep Learning and Machine Learning Techniques for Banking Fraud Detection

Fuad Shamsudeen A
Department of Computer Science
College of Engineering
Karunagappally Kerala, India

Arun Shankar R
Department of Computer Science College
of Engineering Karunagappally
Kerala,India

Akshay S
Department of Computer Science
College of Engineering Karunagappally
Kerala, India

Devanandhan S
Department of Computer Science
College of Engineering Karunagappally
Kerala, India

Renjith S R
Department of Computer Science College
of Engineering Karunagappally Kerala,
India

Swathy S
Department of Computer Science
College of Engineering
Karunagappally Kerala, India

***Abstract*—With the rapid expansion of digital banking, the development of effective fraud detection systems has become crucial.To identify intricate fraudulent patterns in transaction data, we could use deep learning models like Convolutional Neural Networks (CNNs) and Autoencoders in conjunction with ensemble learning models like LightGBM, XGBoost, and CatBoost. Class weight modifications and the creation of synthetic data could be used to address class imbalance, a major problem in fraud detection. By integrating these methods and optimizing performance through optimization algorithms like Bayesian or GridCV coupled with cross folded evaluation, we could ensure a robust and adaptive fraud detection framework.**

This survey analyze various techniques from most promising works in this field, focusing on improving accuracy, reducing false positives and negatives, and ensuring real-time deployment in banking environments. Drawing insights from existing research, we aim to handle imbalanced datasets effectively through class weighting and synthetic data generation, optimizing model performance using Bayesian or GridCV optimization. This approach will enhance fraud detection accuracy and adaptability, minimizing false positives and false negatives.

I. INTRODUCTION

In the age of digital banking, detecting fraud in financial transactions has become essential due to the high financial impact and the rapidly evolving tactics of fraudsters. Traditional systems, often limited by high false positives and static detection methods, struggle to keep up with complex fraud patterns.

The rapid growth of digital banking and online transactions has made financial services more accessible but has also led to a significant rise in fraud, with criminals constantly adapting their tactics to exploit vulnerabilities in transaction systems. Fraud detection in banking is particularly challenging due to the subtle and evolving nature of fraudulent patterns, which are often hidden within vast volumes of legitimate transactions. Unlike traditional anomalies, fraudulent transactions are designed to mimic normal behavior, making detection difficult with simple rule-based or static models. Furthermore, the extreme imbalance between fraudulent and legitimate transactions complicates model training, as most algorithms are biased towards the majority class. Consequently, building a fraud detection system requires sophisticated techniques that can both adapt to new fraud patterns and accurately identify fraudulent activities without interrupting regular banking operations. Taking into account all these factors, the best performing methods are given below.

II. DATASETS

The papers reviewed in this survey utilize various datasets for credit card fraud detection, including the Kaggle Credit Card Fraud Detection Dataset [5], which contains real anonymized transactions with severe class imbalance, and the IEEE-CIS Fraud Detection Dataset [10], offering detailed identity and transaction-based features. Some studies employ PaySim [7], a synthetic financial transaction dataset, to simu- late fraud patterns realistically, while others use ULB's credit card dataset [6], the source of the Kaggle dataset. Additionally, advanced techniques such as GANs and autoencoders are applied to generate synthetic fraud data for enhancing model performance.

III. MACHINE LEARNING TECHNIQUES

The main machine learning and deep learning techniques reviewed in our paper include ensemble learning, traditional classification models, and anomaly detection approaches. These methods have been widely applied in fraud detection to improve accuracy and minimize false positives.

A. Ensemble Learning

Effective machine learning strategies called ensemble learning combine predictions from several models to increase generalisation, accuracy, and robustness. They are particularly effective in fraud detection, where diverse data patterns and class imbalances present significant challenges.

LightGBM: A very effective gradient boosting system made for high-dimensional and large-scale datasets is called Light Gradient Boosting Machine (LightGBM). Instead of splitting trees level-wise, it separates them leaf-wise, which improves optimization and speeds up convergence. This feature makes LightGBM highly scalable and suitable for processing millions of transactional records in real-time.

XGBoost: XGBoost enhances performance by implementing gradient boosting with regularization. It is robust and captures complex patterns in transactional data.

CatBoost: CatBoost handles categorical data efficiently and is resilient to overfitting. It excels in fraud detection scenarios with categorical transaction attributes.

B. Anomaly Detection

Anomaly detection focuses on identifying unusual transaction patterns that deviate from normal banking behavior. Autoencoders are used as the primary deep learning-based anomaly detection technique. During training, the autoencoder learns standard transaction features by minimizing reconstruction errors. When a transaction significantly deviates from these learned patterns, the model generates a high reconstruction error, flagging it as potentially fraudulent. This method effectively identifies rare and complex fraud cases that may escape traditional detection models. By incorporating autoencoders into the fraud detection framework, the project enhances its ability to detect emerging fraud tactics while reducing false negatives in highly imbalanced datasets.

Support Vector Machines (SVMs):SVMs, or supervised learning models, classify data by determining the optimal hyperplane that separates different groups. SVMs categorise transactions as either fraudulent or non-fraudulent in fraud detection. The use of kernel functions allows SVMs to model non-linear relationships in the data, which is particularly important for capturing complex fraud patterns.

Random Forest: Several decision trees are used in the Random Forest ensemble learning technique to categorise transaction data as legitimate or fraudulent. Each tree in the forest is trained using a random subset of the data, and predictions are combined using majority voting. This bagging approach reduces variance and improves model stability, mak- ing Random Forests robust against overfitting.

C. Feature Engineering

SMOTE: By creating synthetic samples for the minority class, the Synthetic Minority Oversampling Technique in- creases the model's sensitivity to fraud cases.

Feature Selection: Techniques like information gain and permutation importance identify high-impact features, improving model efficiency.

IV. DEEP LEARNING TECHNIQUES

Deep learning techniques include Convolutional Neural Networks (CNNs) and autoencoders, to enhance fraud detection in banking transactions. CNNs, typically used for image processing, are adapted in this context to detect complex patterns in sequential transaction data. They excel at capturing spatial and temporal relationships by applying convolutional filters that learn key features indicative of fraudulent behavior. This capability allows the model to recognize subtle anomalies in transaction sequences that traditional models might overlook.

The combination of CNNs and autoencoders creates a robust detection framework. CNNs handle structured features and complex temporal relationships, while autoencoders focus on detecting outliers and unseen fraud patterns. This dual approach addresses both known and emerging fraud tactics effectively. By integrating these models with ensemble learning methods, the project achieves enhanced detection accuracy, reduced false positives, and better generalization across highly imbalanced datasets. This hybrid architecture strengthens the overall system, ensuring a scalable and adaptive fraud detection solution suitable for real-time deployment in banking environments.

A. Convolutional Neural Networks (CNNs)

CNNs are used to detect complex patterns and anomalies in banking transaction data. Although commonly applied to image recognition, CNNs are adapted here to process sequential transaction features. By applying convolutional filters, the model identifies patterns such as unusual spending behaviors or abnormal transaction frequencies. The CNN captures spatial and temporal dependencies within the data, making it well- suited for recognizing subtle fraud indicators that traditional models might miss. Its ability to learn hierarchical feature representations allows for more accurate fraud detection, con- tributing to the project's goal of minimizing false positives and enhancing fraud identification accuracy.

B. Autoencoders

Autoencoders are used in this project for anomaly detection by learning patterns from legitimate banking transactions. A decoder that reconstructs the original input and an en- coder that condenses transaction data into a lower-dimensional representation make up the model. For typical transactions, the autoencoder reduces reconstruction errors during training. When exposed to fraudulent transactions, which deviate from typical patterns, the reconstruction error increases, indicating potential fraud. This approach helps detect complex and previously unseen fraud cases. By integrating autoencoders with other models like CNNs and ensemble classifiers, the system achieves a more comprehensive and accurate fraud detection framework.

C. Recurrent Neural Networks (RNNs)

LSTM and GRU: The use of Gated Recurrent Units (GRUs) and Long Short-Term Memory (LSTM) to identify fraud in sequential transaction data is being investigated. Time- series transaction histories are processed by LSTMs, which are renowned for managing long-term dependencies, by keeping significant patterns and eliminating unnecessary data. This aids in spotting dishonest practices that could surface during several transactions.GRUs, a simpler variant of LSTMs, offer similar functionality with fewer parameters, reducing computational overhead. Both models analyze transaction sequences, capturing temporal dependencies like recurring unusual spending patterns. Their integration enhances the model's ability to detect fraud in real-time while balancing performance and efficiency in handling large-scale banking datasets.

D. Generative Models

Variational Autoencoders (VAEs): Variational Autoen- coders (VAEs) are used in this project for synthetic data generation to address class imbalance in the fraud detection dataset. VAEs learn latent representations of transaction data by encod- ing input features into a compressed vector and decoding them back to reconstruct the original data. During training, VAEs capture key patterns of legitimate transactions. By sampling from the learned latent space, the model generates realistic synthetic samples, particularly for the minority fraud class. This technique boosts the dataset's balance, enabling the fraud detection models to learn better representations and improve detection accuracy while reducing overfitting to the majority class.

GANs: The Generative Adversarial Networks (GANs) can be used to tackle the problem of data imbalance, which is a frequent fraud detection obstacle. A discriminator and a generator neural network make up a GAN. While the discriminator distinguishes between genuine and synthetic samples, the generator generates synthetic transaction data that mimics actual fraud cases. The generator enhances its capacity to generate realistic fraud samples by iterative training, adding a variety of fraudulent cases to the dataset. By increasing the representation of minority fraud cases, improving the model's capacity to identify infrequent fraudulent transactions, and lowering bias in prediction results, this procedure aids in dataset balance.

V. LITERATURE REVIEWS

Hashemi et al. [9](2023) propose a multi-model ensemble approach for fraud detection in banking transactions, combining LightGBM, XGBoost, and CatBoost to improve accuracy. This approach addresses the challenge of class imbalance, a common issue in fraud detection. By combining deep learning and machine learning models into an ensemble framework, the proposed effort expands on this paradigm. By combining the strengths of various algorithms, the goal is to enhance the robustness and accuracy of fraud detection in a highly imbalanced dataset. The ensemble approach helps mitigate the limitations of single models and improves generalization, leading to more reliable and effective fraud detection.

Taha and Malebary [14](2020) present an optimized LightGBM model for fraud detection using Bayesian hyperparameter tuning. The second paper proposes a bagging ensemble of deep learning models to address class imbalance and improve accuracy. This ensemble approach, combined with techniques like SMOTE, is adopted in the proposed project. Deep learning models, particularly CNNs and RNNs, are used for automatic feature extraction, reducing the need for extensive manual feature engineering. By utilizing the advantages of both machine learning and deep learning approaches, the project seeks to achieve reliable and accurate fraud detection while also taking into account pragmatic factors like scalability and processing efficiency.

Alarfaj et al. [2](2022) propose a deep learning-based approach for fraud detection using CNNs and autoencoders. The third paper emphasizes the importance of multi-modal data integration, combining transaction data, user behavior, and device information to enhance detection accuracy. The project adopts this multi-modal approach, leveraging both raw features and derived interactions to capture complex patterns in data. Advanced feature engineering techniques, including data fusion, are employed to optimize model performance. To address class imbalance, a hybrid approach combining undersampling and SMOTE is used. The project evaluates the model using precision, recall, F1-score, and AUC-PR, focusing on the model's ability to detect fraudulent transactions accurately while avoiding false positives. The project also considers practical deployment challenges, such as data synchronization, real-time processing, and computational efficiency, to ensure scalability and real-world applicability.

Alam et al. [1](2020) propose an ensemble approach for credit card default prediction in imbalanced datasets, leveraging a Gradient Boosted Decision Tree (GBDT) as the primary classifier. To tackle the inherent challenges posed by class imbalance, their method incorporates Min- Max normalization to scale features effectively and applies resampling techniques such as Synthetic Minority Oversampling Technique (SMOTE) and K-means clustering to generate a more balanced dataset. By carefully structuring the data preprocessing pipeline, the model ensures that minority class instances are better represented, thereby improving predictive performance. Their approach was tested across multiple datasets, demonstrating notable improvements in accuracy, precision, and recall, especially when trained on balanced data. The study highlights the practical implications of early credit risk assessment, as accurate default prediction enables financial institutions to take proactive measures, mitigating potential losses and optimizing lending strategies.

Ding et al. [8](2023) propose an intro advanced credit card fraud detection model that employs a modified Variational Autoencoder Generative Adversarial Network (VAEGAN) to address the prevalent issue of data imbalance in fraud detection. Unlike traditional oversampling methods, their approach synthesizes diverse and high-quality fraudulent transaction data, significantly enhancing the representation of the minority class. By doing so, the model improves key performance metrics such as precision and F1 score, ensuring a more accurate distinction between fraudulent and legitimate transactions. Their extensive experimental analysis demonstrates that the enhanced VAEGAN framework surpasses conventional oversampling techniques like SMOTE and standard GAN-based models, particularly in capturing rare fraud patterns that often go undetected. This method provides a robust and scalable solution for financial institutions seeking to refine their fraud detection systems, reduce false positives, and enhance overall security measures in digital transactions.

Randhawa et al. [13](2018) propose a hybrid card fraud detection model that integrates AdaBoost and majority voting to leverage the strengths of multiple machine learning algorithms, including Support Vector Machines (SVM) and Random Forest. By combining these classifiers, the ensemble method enhances predictive accuracy and provides a more resilient approach to detecting fraudulent transactions. Their experiments, conducted on both publicly available datasets and real-world financial transaction data, reveal that the majority voting mechanism, coupled with AdaBoost's adaptive learning capabilities, significantly improves model robustness against noisy and imbalanced data distributions. This study underscores the importance of ensemble learning in financial fraud detection, demonstrating how blending diverse classifiers can lead to more reliable predictions. The findings suggest that implementing such hybrid approaches can help financial institutions refine their fraud detection frameworks, reducing operational risks and ensuring more secure transaction environments.

Jemai et al. [12](2024) propose a comparative study on ensemble learning models for detecting fraudulent credit card transactions by applying XGBoost, Random Forest, and Naive Bayes on real (European Union transactions) and synthetic (Sparkov) datasets. The study highlights the effectiveness of ensemble models, especially XGBoost, which performed consistently well on real-world data. The research emphasizes the advantage of ensemble methods in capturing patterns in authentic data, although they showed limitations on synthetic data due to lack of variability. Their approach provides valuable insights into improving credit card fraud detection by balancing ensemble methods and sampling strategies to address data imbalances effectively.

Almazroi and Ayub [3](2023) introduce a sophisticated AI-based framework for online payment fraud detection, utilizing a ResNeXt-embedded Gated Recurrent Unit (RXT) model. The model integrates autoencoders and ResNet (termed EARN) for feature extraction and employs the Jaya optimization algorithm for fine-tuning, achieving high classification accuracy across three datasets. This study underscores the capability of deep learning and ensemble methods to handle data imbalance and temporal dependencies in real-time financial fraud detection, presenting significant advancements in fraud prevention and operational efficiency in financial transactions.

Matin N, Ashtiani and Bijan Raahemi [4](2021) propose a comprehensive literature review focusing on intelligent techniques for detecting fraud in corporate financial statements. The study emphasizes the analysis of machine learning (ML) and data mining (DM) approaches used in detecting fraudulent financial reports, noting that classification techniques are predominantly employed over unsupervised or semi-supervised methods. The review highlights research gaps such as limited exploration of unsupervised learning and the potential of integrating unstructured data like text and audio.

Can Iscan et al. [11](2023) present a fraud detection model for e-wallet transactions utilizing LightGBM. The paper discusses an advanced machine learning solution that achieved a high detection accuracy of 97 percent on data from a major Turkish e-wallet platform. The study underlines the importance of reducing false positives, which decreased significantly from 13,024 to 6,249 using this model. It underscores the efficiency of LightGBM in real-time fraud detection, highlighting its potential for aiding fraud detection teams, especially during high-transaction periods.

VI. COMPARATIVE ANALYSIS

ML models like LightGBM and XGBoost offer computational efficiency and interpretability, making them suitable for structured data. DL models such as CNNs and autoencoders excel at detecting complex patterns but require more computational resources. Hybrid approaches combining ML and DL provide a balance between accuracy and efficiency.

VII. CHALLENGES AND FUTURE DIRECTIONS

Despite advancements, challenges such as interpretability, class imbalance, and scalability remain. Future research should focus on integrating explainable AI techniques, optimizing hybrid models for real-time applications, and addressing evolving fraud tactics.

VIII. SUMMARY OF LITERATURE REVIEW

TABLE I
PERFORMANCE COMPARISON OF MACHINE LEARNING AND DEEP LEARNING TECHNIQUES

Sl No	Title	Authors	Advantages
1	Fraud Detection in Banking Data by Machine Learning Techniques	Hashemi et al	Fast Execution
2	An Intelligent Approach to Credit Card Fraud Detection Using an Optimized Light Gradient Boosting Machine	Taha, Malebary	Memory Efficient
3	Credit Card Fraud Detection Using State-of-the-Art Machine Learning and Deep Learning Algorithms	Alarfaj et al	Flexible Architecture
4	An Investigation of Credit Card Default Prediction in Imbalanced Datasets	Alam et al	Performs well on Imbalanced Dataset
5	Credit Card Fraud Detection Based on Improved Variational Autoencoder Generative Adversarial Network	Ding et al	Highly Scalable
6	Credit Card Fraud Detection Using AdaBoost and Majority Voting	Randhawa et al	Improves accuracy
7	Identifying Fraudulent Credit Card Transactions Using Ensemble Learning	Jemai et al	Highly Scalable
8	Online Payment Fraud Detection Model Using Machine Learning Techniques	Almazroi, Ayub	Efficient real-time processing
9	Intelligent Fraud Detection in Financial Statements Using Machine Learning and Data Mining: A Systematic Literature Review	Matin N.Ashtiani, Bijan Raahemi	Natural Language processing
10	Wallet-Based Transaction Fraud Prevention Through LightGBM With the Focus on Minimizing False Alarms	Can Iscan et al	High Accuracy

IX. CONCLUSION

Fraud detection in financial systems has evolved significantly with the integration of machine learning and deep learning techniques. These methods provide robust solutions for identifying fraudulent activities by analyzing complex patterns and adapting to evolving fraud tactics. Ensemble models like LightGBM and XGBoost offer high accuracy and interpretability, while deep learning architectures such as CNNs and autoencoders excel in handling intricate re- lationships and anomalies within data. Hybrid approaches that combine the strengths of both paradigms present a balanced solution, addressing challenges like class imbalance and scalability. Despite these advancements, issues such as model interpretability, computational efficiency, and real-time applicability remain open for improvement. Future research should focus on developing explainable AI models and enhancing their ability to generalize across diverse datasets. By leveraging these innovations, the next generation of fraud detection systems can ensure enhanced security, reduced false positives, and improved trust in financial transactions.

REFERENCES

[1] Talha Mahboob Alam, Kamran Shaukat, Ibrahim A. Hameed, Suhuai Luo, Muhammad Umer Sarwar, Shakir Shabbir, Jiaming Li, and Matloob Khushi. An investigation of credit card default prediction in the imbalanced datasets. IEEE Access, 8:201173–201198, 2020.

[2] 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, 12:890–902, 2022.

[3] Abdulwahab Ali Almazroi and Nasir Ayub. Online payment fraud detection model using machine learning techniques. IEEE Access, 11:137188–137203, 2023.

[4] Matin N. Ashtiani and Bijan Raahemi. Intelligent fraud detection in financial statements using machine learning and data mining: A systematic literature review. IEEE Access, 10:72504–72525, 2022.

[5] Kaggle Community. Credit card fraud detection dataset. https://www.kaggle.com/mlg-ulb/creditcardfraud, 2016. Accessed: 2024-11-06.

[6] Kaggle Community. Ulb credit card dataset. https://www.kaggle.com/mlg-ulb/creditcardfraud, 2016.Accessed: 2024-11-06.

[7] Kaggle Community. Paysim synthetic financial transactions dataset. https://www.kaggle.com/datasets/mtalaltariq/paysim-data/code, 2023. Accessed: 2024-11-06.

[8] Yuanming Ding, Wei Kang, Jianxin Feng, Bo Peng, and Anna Yang. Credit card fraud detection based on improved variational autoencoder generative adversarial network. IEEE Access, 11:83680–83691, 2023.

[9] S. K. Hashemi, S. L. Mirtaheri, and S. Greco. Fraud detection in banking data by machine learning techniques. IEEE Access, 11:1250–1265, 2023.

[10] Addison Howard, Bernadette Bouchon-Meunier, IEEE CIS, inversion, John Lei, Lynn@Vesta, Marcus2010, and Prof. Hussein Abbass. Ieee-cis fraud detection. https://kaggle.com/competitions/ieee-fraud-detection, 2019. Kaggle.

[11] Can Iscan, Osman Kumas, Fatma Patlar Akbulut, and Akhan Akbulut. Wallet-based transaction fraud prevention through lightgbm with the focus on minimizing false alarms. IEEE Access, 11:131465–131474, 2023.

[12] Jaber Jemai, Anis Zarrad, and Ali Daud. Identifying fraudulent credit card transactions using ensemble learning. IEEE Access, 12:54893–54900, 2024.

[13] Kuldeep Randhawa, Chu Kiong Loo, Manjeevan Seera, Chee Peng Lim, and Asoke K. Nandi. Credit card fraud detection using adaboost and majority voting. IEEE Access, 6:14277–14284, 2018.

[14] A. A. Taha and S. J. Malebary. An intelligent approach to credit card fraud detection using an optimized light gradient boosting machine. IEEE Access, 8:12345–12355, 2020.

[1]–[14]