Published by :
https://www.ijert.org/
An International Peer-Reviewed Journal

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 08 , August - 2026

Comparative Analysis of Machine Learning, Deep learning and Automated Machine Earning Techniques for Credit Card Fraud Detection

[1]Jitender Kumar, [2]Bharti, [3]Nisha Rani
[1] PhD Scholar, Northern Institute for Integrated Learning in Management University Kaithal Haryana India
[2] Assistant Professor, Ganga Institute of Technology & Management Kablana Jhajjar, India
[3] PhD Scholar, Jagannath University Kablana Jhajjar Haryana India

Abstract - The usage of credit cards has risen substantially due to the quick development of the use of digital payments and online banking facilities, which has led to an increase in fraudulent transactions. Due to extremely unbalanced transaction data, changing fraud trends, and the requirement for precise real-time detection, credit card fraud detection has grown to be a significant challenge. The performance of fraud detection has been improved by recent developments in machine learning (ML), deep learning (DL), and automated machine learning (AutoML).

Modern ML, DL, and AutoML techniques for credit card fraud detection are compared in this paper. Deep Learning models like Convolutional Neural Networks (CNNs) are contrasted with traditional machine learning methods like Logistic Regression, Decision Tree, Random Forest, Support Vector Machine, K-Nearest Neighbours, and XGBoost. The article also highlights the advantages of AutoML systems, namely in terms of automating feature selection, algorithm selection, and hyperparameter optimization, which reduces human labor while maintaining high prediction accuracy.

The widely utilised European credit card transaction dataset, which comprises 284,807 transactions with only 492 fraudulent cases—a severely unbalanced classification problem—is employed in the studies under analysis. Accuracy, Precision, Recall, F1-score, and Area Under the ROC Curve (AUC) are used to assess model performance. The results demonstrate that by reaching detection accuracy near 99.9%, high AUC values, and reduced false-negative rates, advanced DL and AutoML algorithms beat several traditional ML methods.

Overall, the review comes to the conclusion that combining AutoML with cutting-edge Deep Learning methods provides a dependable, scalable, and effective framework for real-time credit card fraud detection. Future studies should concentrate on creating explainable and hybrid AI models that can manage changing fraud patterns, enhance model interpretability, and sustain high detection performance in actual financial settings.

Keywords: XGBoost, Artificial Neural Network (ANN), Convolution Neural Network (CNN), Machine Learning, Deep Learning, Automated Machine Learning (AutoML), Fraud Analytics, Class Imbalance, and Financial Security.

1. INTRODUCTION

Due to their convenience, quickness, and ease of use for both online and offline purchases, credit cards have emerged as one of the most widely used payment methods. The rapid adoption of digital banking, e-commerce platforms, mobile payment applications, and contactless payment technology has significantly changed the global financial environment. By facilitating safe, quick, and cashless payments across international borders, these technology developments have streamlined financial transactions. As the number of credit card users and electronic transactions increases, financial institutions manage millions of transactions daily. Banks, payment service providers, retailers, and regulatory bodies are all very concerned about detecting credit card fraud since, although this digital transformation has boosted customer convenience and company efficiency, it has also raised the possibility of financial fraud.

Unauthorized or unlawful transactions carried out with stolen, cloned, or counterfeit credit cards or compromised card information are referred to as credit card fraud. To take advantage of weaknesses in payment systems, fraudsters use a variety of strategies, including identity theft, phishing assaults, card-not-present (CNP) fraud, account takeover, skimming, and synthetic identity fraud.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 08 , August - 2026

Financial firms suffer large financial losses, higher operating expenses, legal responsibilities, and reputational harm as a result of these illegal operations. Additionally, consumers who fall prey to fraud frequently suffer from financial difficulties and lose faith in online payment systems. As a result, the banking and financial industries now place a high premium on creating effective and trustworthy fraud detection systems.

In the past, financial institutions used manual verification procedures and rule-based systems to identify fraudulent transactions. Predefined rules and thresholds, such as abnormally high transaction amounts or transactions coming from unknown locations, are applied by these systems. Rule-based downsides have a number of a number of drawbacks have a number of drawbacks. They produce a lot of false alerts, frequently miss complex or previously undetected fraudulent behaviors, and need constant manual updating to account for new fraud tactics. The need for more intelligent and adaptive procedures is underscored by the fact that standard methods are unable to give precise and real-time detection as fraud patterns change frequently.

Because machine learning (ML) can learn transaction patterns directly from past data and detect suspicious activity without relying exclusively on manually specified rules, it has become a potent option for credit card fraud detection. Supervised learning techniques like Logistic Regression, Decision Tree, Random Forest, Support Vector Machine (SVM), Extreme Gradient Boosting (XGBoost), and Extreme Learning Machine (ELM) have been widely employed for fraud classification. By learning intricate decision limits, these algorithms automatically differentiate between legal and fraudulent transactions based on a variety of transaction parameters. They are ideal for practical fraud detection applications because of their capacity to increase prediction accuracy through data-driven learning.

Due to its exceptional capacity to model extremely complicated and nonlinear interactions inside large-scale transaction datasets, Deep Learning (DL) approaches have drawn a lot of interest in recent years. Without requiring a lot of manual feature engineering, deep learning architectures like Artificial Neural Networks (ANN), Deep Neural Networks (DNN), Convolutional Neural Networks (CNN), and recurrent learning models automatically extract meaningful representations from unprocessed transaction data. These models can spot subtle behavioral traits and hidden fraud trends that traditional machine learning algorithms can miss. Deep learning methods have therefore demonstrated potential in improving fraud detection accuracy, particularly in large and complex financial datasets.

Despite these developments, the extremely unbalanced character of transaction databases remains one of the biggest obstacles to credit card fraud detection. Genuine transactions make up the majority of the dataset in real-world financial systems, with fraudulent transactions accounting for a very tiny percentage of the total transaction volume. Classification models are frequently biased toward the majority class as a result of this imbalance, which makes it difficult to identify fraudulent activity. As a result, drawing conclusions based only on total classification accuracy may be deceptive. More sophisticated evaluation metrics like as Precision, Recall, F1-Score, Area Under the Receiver Operating Characteristic Curve (AUC-ROC), Matthews Correlation Coefficient (MCC), and Fraud Detection Rate provide a more comprehensive assessment of the model's effectiveness. Additionally, data balancing approaches including cost-sensitive learning, undersampling, Adaptive Synthetic Sampling (ADASYN), and Synthetic Minority Oversampling Technique (SMOTE) are widely employed to assist the identification of minority-class fraud scenarios.

In recent years, Automated Machine Learning (AutoML) has gained popularity as a way to simplify the development of sophisticated fraud detection systems. Among the machine learning pipeline operations that AutoML automates are data preprocessing, feature engineering, model selection, hyperparameter optimization, and performance evaluation.. AutoML helps academics and practitioners create reliable, scalable, and high-performing predictive models in a shorter development cycle by eliminating manual involvement and computational work. The growing use of AutoML has opened up new possibilities for enhancing the effectiveness of fraud detection while preserving competitive prediction performance.

Inspired by these advancements, this study offers a thorough comparison of AutoML, Deep Learning, and Machine Learning methods for detecting credit card fraud. The study uses a number of evaluation indicators to assess the effectiveness of several classification algorithms using the benchmark European credit card transaction dataset. The objective is to find the most accurate, reliable, and computationally efficient way to detect fraudulent transactions while lowering false positives. The findings of this study should assist researchers and financial institutions in selecting intelligent models suitable for real-time, large-scale credit card fraud detection systems.

Table 1: Automated Machine Learning, Deep Learning, and Machine Learning Comparison for Credit Card Fraud Detection

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 08 , August - 2026

Paradigm	Advantages	Limitations	Optimal Use Cases
Machine Learning (ML) (Logistic Regression, Decision Tree, Random Forest, SVM, XGBoost, ELM)	High interpretability (particularly LR and DT), efficient on structured tabular data, relatively low processing cost, faster training and inference, well-established techniques.	Requires human feature engineering, has a limited capacity to capture complex nonlinear interactions, and frequently requires manual hyperparameter adjustment. Performance may deteriorate on severely imbalanced data.	Baseline fraud detection systems, transaction classification, banking risk assessment, credit card fraud detection, and real-time scoring with constrained computational resources.
Deep Learning (DL) (ANN, DNN, CNN)	Automatically learns complicated feature representations, effectively captures nonlinear transaction patterns, high detection accuracy, enhanced Recall and F1-score, appropriate for large-scale datasets.	Requires a lot of labeled data, is computationally demanding, takes longer to train, has limited interpretability ("black-box" models), and requires more technology.	Complex financial transaction modeling, behavioral analysis, anomaly identification, large-scale fraud detection, and real-time transaction monitoring .
Automated Machine Learning (AutoML) (JAD, Auto-WEKA, TPOT, H2O AutoML)	By automating preprocessing, feature selection, model selection, and hyperparameter tweaking, it reduces dependence on domain expertise, expedites model development, and often achieves competitive performance.	Reduced user control over the optimization process, high computational cost during automated search, restricted model selection transparency, and scalability dependent on available	Financial decision support systems, automated analytics, comparative model evaluation, companies with little ML experience, and quick implementation of fraud detection models.

2.LITERATURE REVIEW

The growing prevalence of digital payments, internet banking, and e-commerce transactions has made credit card fraud detection a crucial area of research. Early fraud detection systems generally depended on rule-based approaches and manual verification, which were simple to build but lacked adaptability to developing fraud patterns. Researchers developed Machine Learning (ML) methods including Logistic Regression, Decision Trees, Random Forest, Support Vector Machine (SVM), XGBoost, and Extreme Learning Machine (ELM) to get around these restrictions. Among these, boosting algorithms like XGBoost and ensemble techniques like Random Forest have shown better predictive performance, while ELM has drawn notice for its quick training time and appropriateness for real-time fraud detection. However, the extremely unbalanced structure of credit card transaction statistics frequently affects these models' efficacy.

Because Deep Learning (DL) techniques can automatically understand intricate and nonlinear transaction patterns, they are being used more and more to increase the accuracy of fraud detection. Artificial Neural Networks (ANN), Deep Neural Networks (DNN), and Convolutional Neural Networks (CNN) have shown considerable gains in spotting fraudulent transactions compared to several classic ML techniques. To improve the identification of minority-class fraud cases, researchers have also used class imbalance handling strategies like SMOTE, ADASYN, and cost-sensitive learning. These techniques have proven successful in lowering the possibility of incorrectly identifying fraudulent transactions while increasing recall, F1-score, and overall classification performance.

More recently, Automated Machine Learning (AutoML) frameworks like Just Add Data (JAD), Auto-WEKA, TPOT, and H2O AutoML have automated key stages of the machine learning pipeline, such as data preparation, feature selection, model selection, and hyperparameter tuning. These frameworks have reduced development time and expert intervention requirements while achieving competitive prediction performance. Direct comparisons are challenging because the majority of current research evaluates ML, DL, and AutoML algorithms individually using various datasets, preprocessing methodologies, and assessment

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 08 , August - 2026

measures. Consequently, in order to identify the most uniform uniform uniform uniform standardized comparison approach for credit assessment.

Table2 : Review of Credit Card Fraud Detection Methods in the Literature

Author(s) & Year	Title of the Paper	Techniques Used	Key Findings	Limitations
Lin & Jiang (2021)	Credit Card Fraud Detection with Auto encoder and Probabilistic Random Forest	Probabilistic Random Forest with Auto Encoder	Enhanced fraud detection by the extraction of low-dimensional features prior to categorization.	Feature representation determines performance; real-time computing is costly.
Khan et al. (2021)	Credit Card Fraud Detection Using Artificial Neural Network	KNN,SVM, and ANN	ANN outperformed conventional techniques in fraud classification.	Sensitivity to unbalanced datasets and a high false positive rate..
Ileberi et al. (2022)	A Machine Learning Based Credit Card Fraud Detection Using GA Algorithm for Feature Selection	Random Forest, Genetic Algorithm, and Logistic Regression	Feature selection decreased processing time and increased classification accuracy.	GA may not be able to swiftly adjust to changing fraud tendencies and increases computing complexity.
Alarfaj et al. (2022)	Credit Card Fraud Detection Using State-of-the-Art Machine Learning and Deep Learning Algorithms	DNN, Random Forest, and XGBoost	Superior detection performance was attained by XGBoost and Deep Learning.	Insufficient testing on real-world streaming data and a lack of explainability
Jiang et al. (2023)	Credit Card Fraud Detection Based on Unsupervised Attentional Anomaly Detection Network	Unsupervised Learning and Attention Mechanism	Effective in discovering previously undiscovered fraud patterns.	Decreased interpretability and increased training complexity.
Verma & Dhar (2024)	Credit Card Fraud Detection: A Deep Learning Approach	Autoencoder and Deep Learning	Tackled issues like class disparity.	Restricted capacity for explanation and reliance on substantial training data.

3. RESEARCH GAP

- Current research focuses on either AutoML or Deep Learning separately rather than providing a thorough comparison of Machine Learning, Deep Learning, and AutoML under identical experimental settings.
- Because deep learning research do not use automated optimization approaches and current AutoML studies emphasize standard ML algorithms, there is still limited integration of AutoML with sophisticated deep learning models.
- Class imbalance is mostly addressed by current techniques, but more advancement are required to reliably detect fraudulent transactions while reducing false alarms and overlooked fraud situations.
- Despite the achievement of great detection performance, little study has been done on the practical deployment, scalability, and computational efficiency of fraud detection models in real-time financial applications.

4. PROBLEM STATEMENT

- A thorough comparison of Machine Learning, Deep Learning, and AutoML models utilizing a single experimental framework is absent from previous research.
- AutoML and state-of-the-art Deep Learning techniques for credit card fraud detection are still not fully integrated.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 08 , August - 2026

- The extremely uneven nature of credit card transaction datasets continues to reduce fraud detection performance due to a rise in false positives and false negatives.
- The computational efficiency, scalability, and real-time applicability of current fraud detection models for real-world financial systems are only partially evaluated.

5. PROPOSED SOLUTION

This study suggests a Unified Comparative Credit Card Fraud Detection Framework that combines Machine Learning (ML), Deep Learning (DL), and Automated Machine Learning (AutoML) into a single experimental pipeline in order to address the shortcomings found in current credit card fraud detection systems. The suggested methodology allows a methodical evaluation of ML, DL, and AutoML models under the same experimental settings, in contrast to earlier research that assesses these methods separately.

The first step in the suggested approach is to get a benchmark dataset of European credit card transactions. Data preprocessing, which includes feature scaling, data cleaning, and normalization, comes next. Appropriate resampling techniques, such as SMOTE or ADASYN, are employed prior to model training to solve the issue of highly unbalanced transaction data. The quality of input features is then enhanced by feature engineering and feature selection.

Several Machine Learning models (Logistic Regression, Decision Tree, Random Forest, Support Vector Machine, and XGBoost), Deep Learning models (Artificial Neural Network and Convolutional Neural Network), and AutoML frameworks (e.g., H2O AutoML or AutoGluon) are then trained using the processed dataset. All models are evaluated using the same datasets using standardized evaluation criteria, including Precision, Recall, F1-Score, AUC-ROC, training time, inference time, and computing efficiency.

A comparison analysis is then used to identify the best reliable, scalable, accurate, and computationally efficient model suitable for real-time credit card fraud detection in financial systems.

Comparative Review Framework

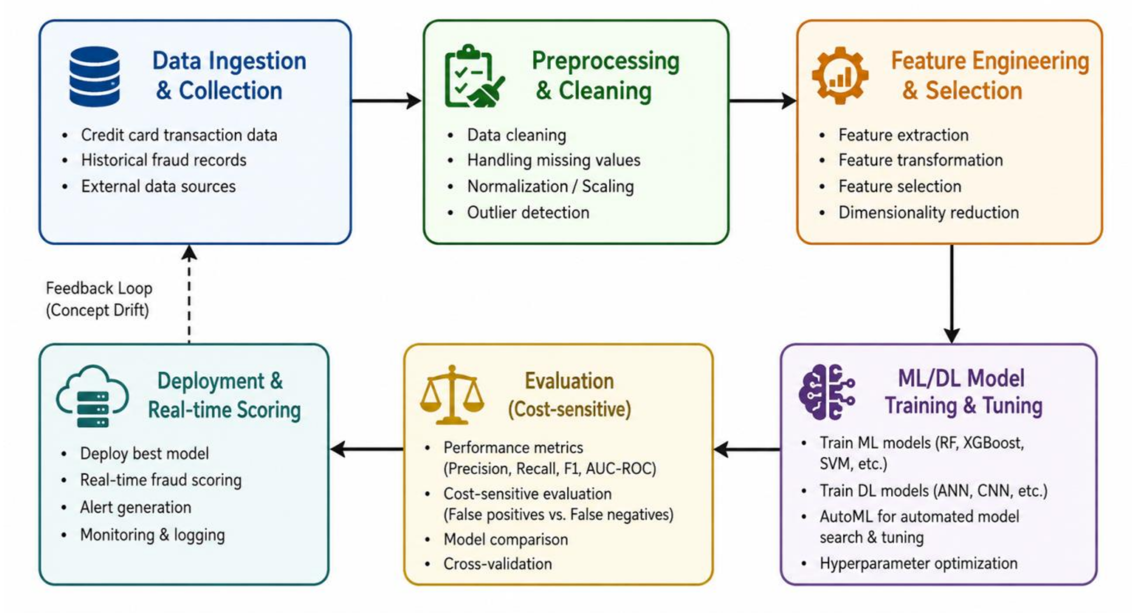


Figure 4.1:Proposed Architecture for Hybrid Credit Card Fraud Detection

The following stages make up the suggested framework:

1. Data Ingestion and Collection: Gather historical fraud records, the benchmark European credit card transaction dataset, and other pertinent data sources needed for fraud detection.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 08 , August - 2026

2. **Data Preprocessing and Cleaning**: Perform data cleaning, handle missing values, normalize and scale the data, and find outliers in order to improve data quality and prepare the dataset for model training.

3. **Feature Engineering and Feature Selection**: To minimize dimensionality and boost model performance, extract significant features, conduct out feature transformation, and identify the most pertinent characteristics using statistical or model-based methods..

4. ML/DL Model Training and Hyperparameter Tuning: Develop and train a range of machine learning models (Logistic Regression, Decision Tree, Random Forest, Support Vector Machine, and XGBoost), deep learning models (Artificial Neural Network and Convolutional Neural Network), and AutoML frameworks (such as H2O AutoML or AutoGluon). Reduce human intervention and improve prediction performance by using automated tuning strategies to optimize model hyperparameters.

5. Model Evaluation: Use cross-validation and cost-sensitive evaluation to assess the trained models. Evaluate model performance using Precision, Recall, F1-Score, AUC-ROC, false positive and false negative rates, and compare the computational efficiency of various models.

6. Deployment and Real-Time Scoring: Choose the top-performing model based on computational efficiency and predictive accuracy, implement it for real-time credit card fraud detection, produce fraud alerts, keep an eye on system performance, and include a feedback loop to deal with concept drift and keep the model getting better.

Algorithm 1: A Unified Comparative Framework for Identifying Credit Card Fraud

Credit Card Transaction Dataset (D) is the input.

Result: The Best Fraud Detection Model (Mbest)

1. Open dataset D, which contains credit card transactions.

2. Preprocess the data by cleaning, normalizing, and scaling the features.

3. To address class imbalance, use SMOTE/ADASYN.

4. Carry out feature selection and engineering.

5. Develop models for AutoML, Deep Learning, and Machine Learning.

6. Conduct cross-validation and optimize the model's hyperparameters.

7. Evaluate each model using precision, recall, F1-score, AUC-ROC, training time, and computing efficiency.

8. Evaluate how well ML, DL, and AutoML models perform.

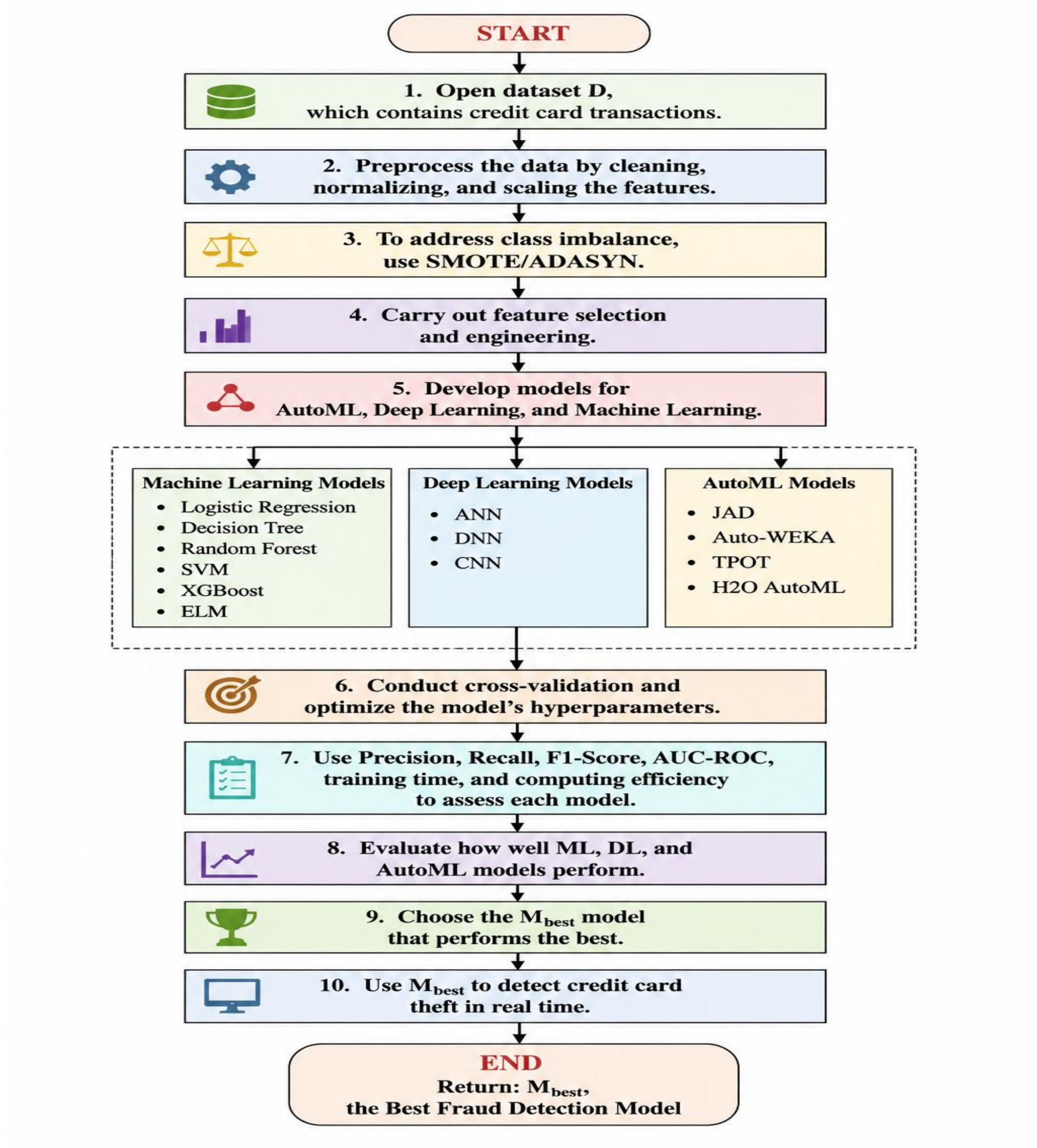
9. Choose the Mbest model that performs the best.

10. Use Mbest to detect credit card theft in real time.

Return: Mbest, the Best Fraud Detection Model

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 08 , August - 2026



6. APPLICATIONS OF FRAUD DETECTION

6.1.Financial Institution and Banking

Banks and other financial institutions frequently utilize credit card fraud detection systems to instantly spot unusual transactions. These systems enhance the general security of customer accounts and lessen monetary losses brought on by fraudulent activity.

6.2. Online Shopping Portals

Fraud detection systems are used by online retailers to safeguard digital payments and stop illegal transactions. Before payments are finalized, these systems examine consumer transaction patterns and spot questionable activity.

6.3. Digital Payments and Mobile Banking

Fraud detection solutions are crucial for tracking transactions as the use of digital wallets and mobile banking apps grows. They assist in identifying anomalous payment patterns, stop illegal access, and offer consumers safe online payment services.

6.4. Risk management and cyber security

Cyber security frameworks also make use of fraud detection tools. They assist companies in spotting fraudulent activity, lowering financial risks, and bolstering defenses against identity theft, account takeover fraud, and cyberattacks.

6.5. Compliance with Government and Regulations

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 08 , August - 2026

Fraud detection systems are used by government agencies and regulatory bodies to keep an eye on financial crimes and make sure financial regulations are being followed. These systems help identify illicit transactions, financial fraud, and money laundering.

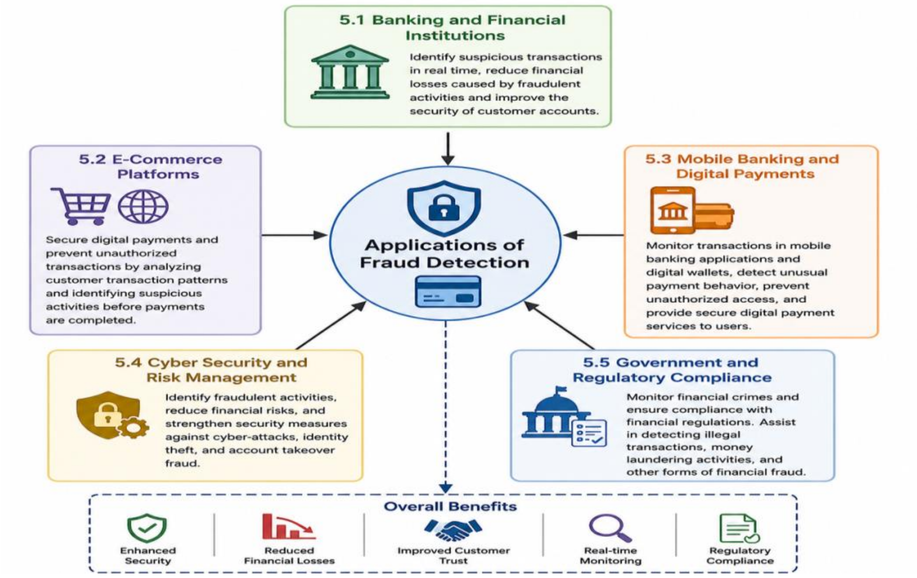


Figure 2: Fraud Detection System Application Domains

7. FUTURE SCOPE OF FRAUD DETECTION

7.1.Hybrid Model Development

Future studies could concentrate on integrating AutoML, Deep Learning, and Machine Learning methods into a single hybrid model. By combining the advantages of several methods, these models can lower false-positive rates and increase the accuracy of fraud detection.

7.2. Systems for Fraud Detection in Real Time

Real-time fraud detection systems are becoming more and more necessary as the number of digital transactions rises. Future systems ought to be able to quickly analyze massive amounts of transactions and spot fraudulent activity before money is lost.

7.3. XAI, or Explainable Artificial Intelligence

Many sophisticated fraud detection programs operate as "black boxes," making it challenging to comprehend their conclusions. Explainable AI should be the key emphasis of future research to increase the transparency, comprehensibility and dependability of fraud detection systems for both financial institutions and customers.

7.4. Federated Education and Protection of Privacy

Federated Learning can be used by future fraud detection systems to train models without disclosing private client information. This strategy will enhance privacy protection while enabling businesses to develop extremely precise fraud detection models.

7.5. Fraud Detection Using Graphs

Hidden relationships between users, merchants, and transactions can be found using Graph Neural Networks (GNNs) and network analysis techniques. This will make it easier to identify sophisticated fraudulent activity and organized fraud networks.

7.6. Self-Learning and Adaptive Systems

Future fraud detection systems should be able to continuously learn from new transaction data and automatically adapt to changing fraud patterns. This will enhance their capacity to identify new fraud strategies and sustain excellent performance over time.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 08 , August - 2026

7.7. Including New Technologies

To improve security, scalability, and efficiency, fraud detection systems can be coupled with technologies like block chain, big data analytics, artificial intelligence, and cloud computing. These technologies will play a major role in the next generation of advanced fraud detection systems.

8. CONCLUSION

The risk of credit card fraud has greatly increased due to the quick development of digital payment systems and online financial transactions, making fraud detection a crucial task for financial institutions. This paper gives a comparative examination of Machine Learning, Deep Learning, and AutoML approaches for detecting fraudulent credit card transactions.

By assessing several models within a same experimental framework, the study aims to address important issues like class imbalance, false positive rates, and model optimization. To provide a fair comparison between the chosen approaches, a variety of preprocessing techniques, class balance strategies, and performance evaluation measures are used.

The comparative analysis enables the identification of the most effective fraud detection model in terms of accuracy, precision, recall, F1-score, and ROC-AUC performance. The research demonstrates that advanced data-driven approaches can significantly improve fraud detection capability while reducing financial losses and enhancing transaction security.

Additionally, the use of AutoML approaches makes fraud detection systems more effective and scalable by reducing the reliance on manual feature engineering and hyperparameter tuning. The study's conclusions offer banks, financial organizations, payment gateways, and researchers useful information for creating clever and trustworthy fraud detection systems.

All things considered, the proposed framework improves the effectiveness of credit card fraud detection systems and establishes the foundation for future research in deep learning-based security applications, explainable artificial intelligence, and real-time fraud detection.

REFERENCES

[1] "Credit Card Fraud Detection with Automated Machine Learning Systems," Applied Artificial Intelligence, vol. 36, no. 1, pp. 1–17, 2022; V. Plakandaras, P. Gogas, T. Papadimitriou, and I. Tsamardinos.
[2] "Credit Card Fraud Detection Using State-of-the-Art Machine Learning and Deep Learning Algorithms," IEEE Access, vol. 10, pp. 39700–39715, 2022, F. K. Alarfaj, I. Malik, H. U. Khan, N. Almusallam, M. Ramzan, and M. Ahmed.
[3] "Calibrating Probability with Undersampling for Unbalanced Classification," A. Dal Pozzolo, O. Caelen, R. A. Johnson, and G. Bontempi, IEEE Symposium Series on Computational Intelligence, 2015.
[4] "Neural Fraud Detection in Credit Card Operations," D. Dorronsoro, F. Ginel, C. Sanchez, and C. Cruz, IEEE Transactions on Neural Networks, vol. 8, no. 4, pp. 827–834, 1997.
[5] European Journal of Operational Research, vol. 247, no. 1, pp. 124–136, 2015; S. Lessmann, B. Baesens, H. V. Seow, and L. C. Thomas, "Benchmarking State-of-the-Art Classification Algorithms for Credit Scoring."
[6] W. Ngai, Y. Hu, Y. Wong, Y. Chen, and X. Sun, "The Application of Data Mining Techniques in Financial Fraud Detection: A Classification Framework and Literature Review," Decision Support Systems, vol. 50, no. 3, pp. 559–569, 2011.
[7] A. Dal Pozzolo, O. Caelen, Y. Le Borgne, S. Waterschoot, and G. Bontempi, "Learned Lessons in Credit Card Fraud Detection from a Practitioner Perspective," Expert Systems with Applications, vol. 41, no. 10, pp. 4915–4928, 2014.
[8] "Sequence Classification for Credit Card Fraud Detection," Expert Systems with Applications, vol. 100, pp. 234–245, 2018; N. Jurgovsky, M. Granitzer, K. Ziegler, S. Calabretto, P. Portier, L. He-Guelton, and O. Caelen.
[9] C. C. Aggarwal, Outlier Analysis, Cham, Switzerland: Springer, 2017, 2nd ed.
[10] Deep Learning, I. Goodfellow, Y. Bengio, and A. Courville. MIT Press, Cambridge, MA, USA, 2016.
[11] XGBoost: A Scalable Tree Boosting System, T. Chen and C. Guestrin, Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, San Francisco, USA, 2016, pp. 785–794.
[12] "SMOTE: Synthetic Minority Over-Sampling Technique," N. V. Chawla, K. W. Bowyer, L. O. Hall, and W. P. Kegelmeyer, Journal of Artificial Intelligence Research, vol. 16, pp. 321–357, 2002.
[13] H. Han, W. Y. Wang, and B. H. Mao, "Borderline-SMOTE: A New Over-Sampling Method in Imbalanced Data Sets Learning," International Conference on Intelligent Computing, Hefei, China, 2005, pp. 878–887.
[14] "Efficient and Robust Automated Machine Learning," M. Feurer et al., Advances in Neural Information Processing Systems (NeurIPS), vol. 28, pp. 2962–2970, 2015.
[15] "TPOT: A Tree-Based Pipeline Optimization Tool for Automating Machine Learning," by R. S. Olson and J. H. Moore, Workshop on Automatic Machine Learning, PMLR, 2016.
[16] "H2O AutoML: Scalable Automatic Machine Learning," E. LeDell and S. Poirier, H2O.ai White Paper, 2020.
[17] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly Detection: A Survey," ACM Computing Surveys, vol. 41, no. 3, pp. 1–58, 2009.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)