iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** I **Month of publication:** January 2026

DOI: https://doi.org/10.22214/ijraset.2026.74389

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue I Jan 2026- Available at www.ijraset.com

A Novel Hybrid Algorithms for Credit Card Fraud Detection in Banking- A Review

Shashank Poddar[1], Dr. Anshu Tiwari[2]
[1]*Research Scholar,* [2]*Assistant Professor, Bansal Institute of Science and Technology, Bhopal (M.P)*

Abstract: ***Fraud detection in the financial sector, particularly in credit card transactions, is a critical issue that requires efficient and accurate models to safeguard against financial losses. Traditional methods of fraud detection are often limited by their ability to process complex and large datasets in real-time. Hybrid algorithms, which combine multiple techniques like machine learning, deep learning, and ensemble methods, have emerged as a solution to this challenge. This paper reviews the application of hybrid models in credit card fraud detection, highlighting their advantages, including improved accuracy, better generalization, and the ability to handle imbalanced data. It discusses deep learning architectures such as neural networks, convolutional neural networks (CNNs), and long short-term memory (LSTM) networks, and how these models capture intricate patterns in fraud detection tasks. The paper also compares hybrid algorithms with traditional machine learning models, emphasizing the enhanced performance and operational efficiency of hybrid approaches. Furthermore, it explores the importance of data preprocessing, feature engineering, and performance metrics in evaluating fraud detection models. The findings indicate that hybrid algorithms have significant potential in improving fraud detection systems, making them a promising avenue for future research and application.***

Keywords: Credit card fraud, fraud detection, hybrid algorithms, machine learning, deep learning, ensemble methods, neural networks, CNN, LSTM, feature engineering, data preprocessing, evaluation metrics.

I. INTRODUCTION

Credit card fraud is a pervasive issue in the global financial sector, and it continues to evolve as technology advances. It occurs when an individual or group illegally obtains and uses someone else's credit card information to make unauthorized purchases or transactions. The types of fraud include card-not-present fraud (where the physical card is not used), card-present fraud (where the physical card is used in transactions), and identity theft, among others. The methods of committing fraud have become more sophisticated over the years, ranging from skimming and phishing attacks to data breaches and hacking.With the increasing reliance on digital payments and online shopping, credit card fraud has risen exponentially. According to various studies and reports, the financial impact of credit card fraud is substantial, costing banks, consumers, and merchants billions of dollars annually. In the United States alone, the cost of credit card fraud was estimated to be over $28 billion in 2021, with similar trends observed worldwide. As the methods of fraud evolve, there is a growing urgency for banks to adopt innovative approaches to protect customers and financial institutions from these malicious activities.

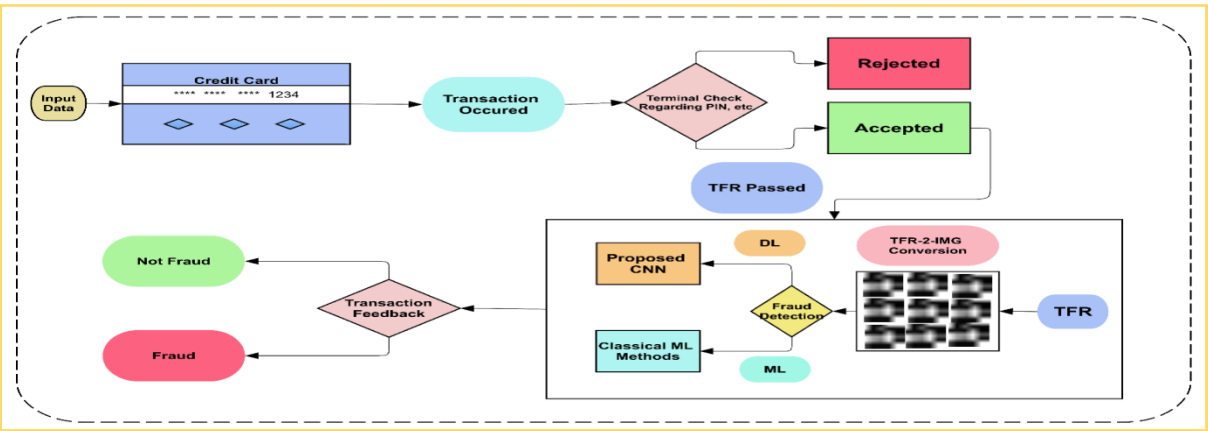


Figure 1: AI enabled Credit Card Fraud Detection (Abdullah et al., 2022)

A. *Impact of Credit Card Fraud on the Banking Sector*

The banking sector is the primary target of credit card fraud, and the consequences are far-reaching. Fraudulent activities can result in direct financial losses, but the long-term impact extends beyond that. The costs associated with fraud detection, recovery, and the implementation of preventive measures are significant. Fraudulent transactions can lead to legal and regulatory challenges, as financial institutions are often required to refund customers for unauthorized purchases, which further affects their bottom line.Customer trust is one of the most important assets for banks, and fraud can severely damage this trust. When consumers feel that their financial information is not secure, they may choose to switch to competing financial institutions that offer better fraud protection. Additionally, banks may suffer from reputational damage if fraud incidents are handled poorly or if fraudulent activities go unnoticed for extended periods. In a highly competitive financial ecosystem, maintaining customer loyalty while minimizing fraud is crucial for sustaining market share.

B. *The Need for Efficient Credit Card Fraud Detection Systems*

With the rise in online transactions, credit card fraud detection has become a high-priority concern for banks. Traditional fraud detection systems, which are rule-based and rely on predefined patterns of fraudulent behaviour, are becoming increasingly inadequate. These systems struggle to identify new or unknown fraud tactics, as they often depend on historical data and fixed thresholds that cannot adapt to evolving fraud schemes. As a result, false positives (legitimate transactions flagged as fraudulent) and false negatives (fraudulent transactions going undetected) occur frequently, undermining the effectiveness of fraud prevention efforts.

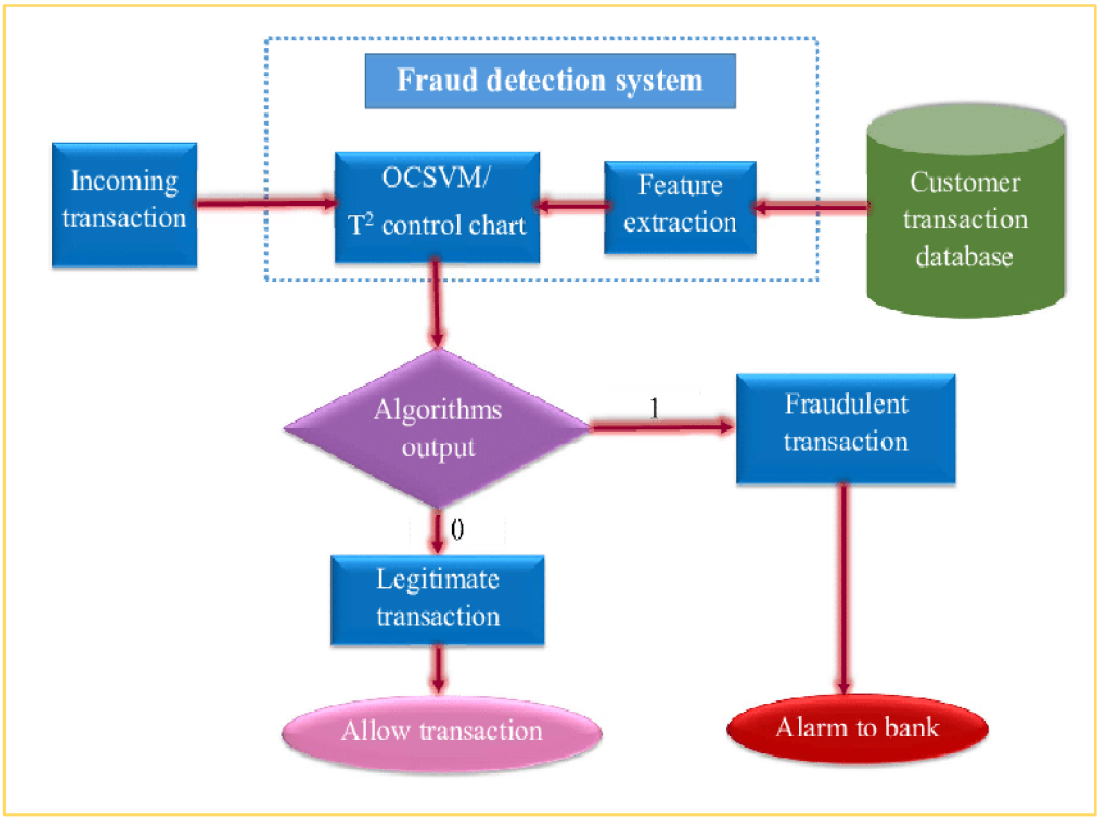


Figure 2: An efficient Fraud Detection mechanism (Phuong et al., 2018)

Real-time fraud detection systems that can instantly analyze transactions and detect anomalies are essential for modern banking systems. To achieve this, machine learning (ML) and artificial intelligence (AI) have emerged as crucial tools, enabling the development of dynamic, self-learning models. Machine learning algorithms can identify patterns and trends in data that are difficult to detect with traditional methods, allowing for more accurate and timely detection of fraud. However, even machine learning systems face challenges, such as handling imbalanced datasets (with far more legitimate transactions than fraudulent ones) and ensuring that models do not overfit to the data.

II. REVIEW OF LITERATURE

The detection of credit card fraud has garnered significant attention in recent years, owing to the increasing frequency of fraudulent activities and the growing need for efficient, automated detection systems.

Various studies have explored the use of traditional methods, statistical techniques, and, more recently, machine learning and hybrid algorithms to tackle this complex problem. Early methods for credit card fraud detection predominantly relied on rule-based systems and statistical models. These traditional approaches typically involved predefined rules or thresholds that flagged unusual transactions based on criteria such as transaction amount, frequency, and location. However, these models often lacked the adaptability required to identify novel fraud patterns, which led to their limited effectiveness in detecting sophisticated fraud schemes (Pandey et al., 2021).With the advent of machine learning, more dynamic and adaptive models began to be developed. Machine learning algorithms are capable of learning from historical data and identifying complex, non-linear relationships between features that might be indicative of fraudulent behaviour.

Research by Lim et al. (2021) highlights the significant role of machine learning algorithms in detecting fraudulent transactions with high accuracy. Among these, decision trees, random forests, and support vector machines (SVM) have been widely used due to their effectiveness in handling large datasets and providing reliable classification results. However, these models are not without limitations, particularly when it comes to handling imbalanced datasets, which is a common issue in fraud detection tasks where fraudulent transactions represent only a small fraction of the total transactions.In response to these challenges, several hybrid algorithms have been proposed to improve the performance of fraud detection systems. A hybrid approach combines multiple models or techniques to leverage their individual strengths and overcome the weaknesses of a single algorithm.

For instance, Kamusweke et al. (2019) proposed a hybrid approach that combines decision trees with neural networks to enhance fraud detection accuracy by capturing both global patterns and local anomalies in the data. Similarly, Thennakoon et al. (2019) utilized ensemble learning methods to combine the strengths of multiple classifiers, improving the system's ability to detect fraud in real-time.Recent advancements in deep learning have further revolutionized the field of credit card fraud detection. Deep learning models, particularly neural networks, have demonstrated remarkable performance in identifying intricate fraud patterns due to their ability to learn complex features from large datasets. Studies such as those by Xie et al. (2021) and Lim et al. (2021) have shown that deep learning models like convolutional neural networks (CNNs) and recurrent neural networks (RNNs) can outperform traditional machine learning models in terms of accuracy and efficiency, especially in handling large-scale and unstructured data.

Moreover, the rise of unsupervised learning techniques has contributed to overcoming the challenges of imbalanced datasets. In many fraud detection scenarios, labelled data is scarce, which makes it difficult to train traditional supervised models effectively. Unsupervised learning algorithms, such as clustering and anomaly detection, offer a viable solution by identifying outliers in the data without relying on labelled examples. According to Barman et al. (2016), unsupervised learning techniques can be particularly useful in detecting new and unknown fraud patterns that do not conform to previously observed behaviours.Despite the advancements, several challenges remain in credit card fraud detection. One of the primary issues is the imbalance between the number of fraudulent and non-fraudulent transactions in the dataset.

This imbalance can lead to biased model performance, where the system is overly focused on predicting the majority class (non-fraudulent transactions) at the expense of detecting fraud. To address this, researchers have proposed various techniques such as oversampling, under sampling, and the use of cost-sensitive learning methods to improve the detection of fraudulent transactions (Padvekar et al., 2016).In addition to imbalanced data, the evolving nature of fraud tactics presents another challenge. Fraudsters continually develop new strategies to circumvent detection systems, making it necessary for fraud detection models to be adaptive and capable of learning from new data. Recent studies have suggested that continuous model retraining and the integration of real-time data streams can help mitigate the impact of changing fraud patterns.

For example, Thennakoon et al. (2019) demonstrated the use of real-time fraud detection systems that update the model periodically to maintain high detection accuracy over time.Furthermore, the interpretability of machine learning models remains a critical issue in the adoption of these technologies for credit card fraud detection. Many complex models, especially deep learning models, operate as black boxes, making it difficult to understand the reasoning behind their predictions. This lack of transparency can be a barrier to trust and acceptance, particularly in regulated industries like banking and finance. To address this, researchers have focused on improving the explainability of models, such as using feature importance analysis and model-agnostic interpretability techniques, to provide insights into how models make decisions.While machine learning, hybrid algorithms, and deep learning have significantly improved the accuracy and efficiency of credit card fraud detection, challenges related to data imbalance, fraud adaptation, and model interpretability remain. Ongoing research in these areas aims to refine detection systems, making them more adaptive, transparent, and capable of identifying emerging fraud patterns.

Future advancements will likely involve the integration of advanced techniques such as reinforcement learning, federated learning, and the use of multi-modal data to further enhance the effectiveness of credit card fraud detection systems.

III. HYBRID ALGORITHMS IN FRAUD DETECTION

Hybrid algorithms have gained significant attention in the field of fraud detection due to their ability to combine the strengths of multiple techniques, leading to improved model performance. These models leverage the advantages of various machine learning, deep learning, and statistical approaches to enhance detection accuracy, robustness, and adaptability. Hybrid algorithms are particularly useful in complex tasks such as credit card fraud detection, where the data is often noisy, imbalanced, and subject to continuous change. By combining multiple methodologies, hybrid models aim to overcome the limitations of individual approaches and provide more accurate, reliable results in detecting fraudulent activities.Ensemble methods are one of the most common types of hybrid algorithms used in fraud detection. These methods combine multiple weak learners to create a stronger, more accurate model. Popular ensemble techniques include Random Forest, Boosting, and Bagging. Random Forest, for example, creates a forest of decision trees, with each tree being trained on a random subset of the data.

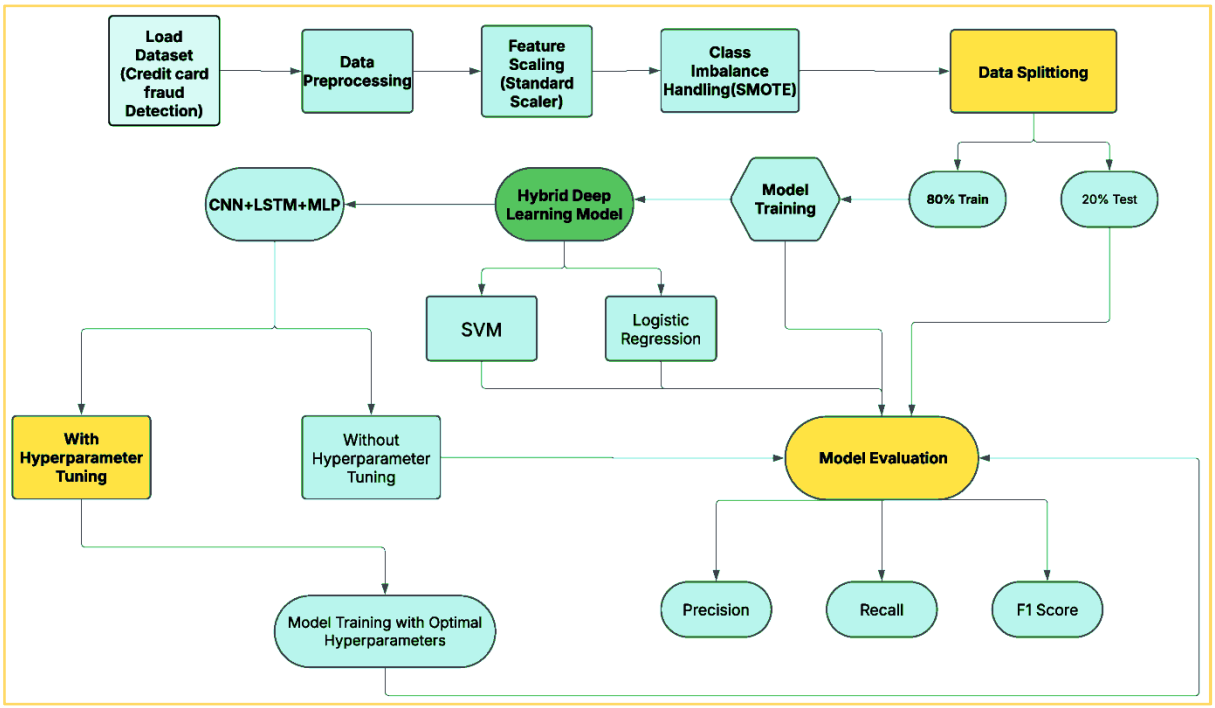


Figure 3: Hybrid Algorithms based Credit card Fraud Detection System (Madiha Jabeen et al., 2025)

The final prediction is based on the majority vote from all trees, which helps to improve generalization and reduce overfitting. Boosting and Bagging methods, on the other hand, focus on iteratively refining predictions by adjusting weights based on errors made in previous rounds, ultimately resulting in a more accurate ensemble model. These methods are particularly useful for handling imbalanced datasets, as they can assign higher weights to the minority class (fraudulent transactions) to ensure they are adequately represented in the model's predictions.Another effective hybrid approach combines traditional machine learning techniques with deep learning methods.

While machine learning algorithms like decision trees and support vector machines are powerful, deep learning models, such as neural networks, are able to capture complex, non-linear relationships in large datasets. By integrating machine learning with deep learning, these hybrid models can benefit from the interpretability and simplicity of traditional techniques while leveraging the advanced capabilities of deep learning to identify intricate patterns that may otherwise go undetected. For instance, a hybrid model might use a machine learning algorithm like a decision tree to preprocess the data or extract features and then feed this information into a deep neural network for final prediction. This combination allows the system to process data more effectively and achieve higher accuracy in fraud detection tasks.

Hybrid clustering and classification algorithms also play a significant role in fraud detection. Clustering algorithms, such as K-means or DBSCAN, can be used to group similar transactions together based on common features, identifying patterns and anomalies within the data. Once the data is grouped into clusters, classification algorithms like decision trees, SVMs, or deep learning models can be applied to label the clusters as either fraudulent or non-fraudulent.

This hybrid approach is particularly effective in scenarios where fraudulent transactions are sparse or evolve over time, as clustering can help uncover hidden patterns that may not be immediately apparent using classification alone. By using clustering as a preprocessing step, the model can more accurately detect novel fraud patterns that do not fit the typical distribution of non-fraudulent transactions.The advantages of hybrid algorithms in fraud detection are numerous. First, they often achieve improved accuracy by combining the strengths of multiple methods, reducing the likelihood of model underperformance. The integration of different techniques allows hybrid models to better generalize across various types of data, making them more robust to new and unseen fraud patterns. Additionally, hybrid models can reduce overfitting, as they are less likely to rely too heavily on any single method that may be prone to overfitting the data.

IV. DEEP LEARNING IN FRAUD DETECTION

Deep learning has revolutionized the field of fraud detection by enabling the automatic learning of intricate patterns within large datasets. Architectures like Neural Networks (NNs), Convolutional Neural Networks (CNNs), and Long Short-Term Memory (LSTM) networks have shown significant promise in detecting fraud. NNs are capable of learning non-linear relationships in data, while CNNs, typically used in image processing, can be adapted to detect fraud in structured data by identifying spatial hierarchies. LSTM networks, a type of Recurrent Neural Network (RNN), excel in tasks involving sequential data and time-series analysis, making them well-suited for detecting fraud over time in transaction datasets.The application of deep learning in fraud detection involves training these models on vast datasets of transactional data, allowing them to automatically identify anomalies that indicate fraudulent activity. These models can detect subtle patterns and complex interactions between features that traditional models might miss. While traditional models rely heavily on manually crafted features, deep learning approaches automatically extract meaningful features from raw data, improving their predictive accuracy and ability to generalize to new, unseen fraud patterns.

Table 1: Comparison of Deep Learning Models and Their Applications in Fraud Detection.

Deep Learning Model	Strengths	Application in Fraud Detection
Neural Networks (NN)	Learn non-linear relationships, flexible architecture	Detects complex fraud patterns and anomalies
Convolutional Neural Networks (CNN)	Excellent for spatial pattern recognition	Can identify hidden fraud patterns in structured data
Long Short-Term Memory (LSTM)	Great for sequential data, captures long-term dependencies	Ideal for detecting fraud in time-series data (e.g., transaction sequences)

This table summarizes the strengths of various deep learning models such as Neural Networks (NN), Convolutional Neural Networks (CNN), and Long Short-Term Memory (LSTM) networks, highlighting their capabilities in detecting complex fraud patterns, analyzing spatial and sequential data, and improving detection accuracy in large datasets.

V. DATASETS AND DATA PREPROCESSING

A. Popular Datasets

Table 2**:** Popular datasets for fraud detection tasks

Dataset	Description	Use Case
European Credit Card Fraud Dataset	Contains anonymized credit card transactions, including both legitimate and fraudulent transactions.	Credit card fraud detection
UCI Machine Learning Repository	A widely used collection containing various datasets for fraud detection across different domains.	General fraud detection tasks
Kaggle Credit Card Fraud Dataset	A dataset from Kaggle with credit card transactions labelled as fraudulent or legitimate.	Used in machine learning competitions for fraud detection

Fraud detection systems, particularly those using machine learning and deep learning techniques, depend significantly on the dataset used for training and evaluation. Below is an overview of popular datasets, pre-processing techniques, and the importance of feature engineering in fraud detection.

B. Data Preprocessing Techniques

Data preprocessing plays a pivotal role in fraud detection by ensuring clean and normalized data for better model performance. Key preprocessing techniques include:

Table 3: Data preprocessing techniques for effective fraud detection.

Pre-processing Technique	Description	Purpose
Normalization	Rescales data to a specific range, ensuring uniformity and preventing feature dominance.	To standardize feature ranges
Missing Value Handling	Deals with incomplete data using techniques like imputation or removal of missing entries.	Ensures model training consistency
Feature Selection	Selects the most relevant features while discarding irrelevant ones.	Enhances model performance
Handling Class Imbalance	Techniques like SMOTE, under sampling, or oversampling are used to balance fraudulent and non-fraudulent transaction data.	Prevents model bias toward majority class

C. Feature Engineering

Feature engineering involves the extraction and creation of domain-specific features that can significantly improve the model's performance. The following table highlights essential feature engineering considerations:

Table 4: Key feature engineering techniques for fraud detection.

Feature Engineering Technique	Description	Purpose
Transaction Time	Extracts patterns based on the time of day or week the transaction occurred.	Identifies unusual activity timings
User Behaviour Patterns	Tracks historical data for users to identify deviations from normal behaviour.	Spot abnormal patterns
Purchase Frequency and Amount	Considers how often a user purchases and the average transaction size.	Detects outliers in spending behaviour
Geolocation and Device Usage	Includes location-based or device information that might reveal suspicious activity.	Identifies abnormal geographic patterns

VI. EVALUATION METRICS FOR FRAUD DETECTION

Evaluation metrics play a crucial role in assessing the performance of fraud detection models. These metrics help determine how well the model identifies fraudulent transactions while minimizing false positives and negatives. Key performance metrics include accuracy, precision, recall, F1-score, and AUC-ROC curve. Accuracy measures the overall correctness of the model, but it may not be sufficient, especially in the case of imbalanced data where fraudulent transactions are a minority.

Precision and recall are more informative, with precision focusing on the proportion of true positives among predicted positives, and recall indicating the proportion of actual positives correctly identified. The F1-score provides a balance between precision and recall, making it an ideal metric when there is a trade-off between the two. The AUC-ROC curve further evaluates the trade-off between true positive rate and false positive rate, which is critical in fraud detection. Additionally, the confusion matrix provides a detailed breakdown of true positives, true negatives, false positives, and false negatives, helping analysts better understand the model's performance. When evaluating hybrid models, which combine multiple algorithms, performance must be assessed not only for accuracy but also for operational efficiency and the ability to handle different types of fraud detection tasks. Benchmarking hybrid models against traditional models helps demonstrate their advantages in terms of robustness, ability to generalize across various fraud patterns, and their efficiency in processing large-scale datasets.

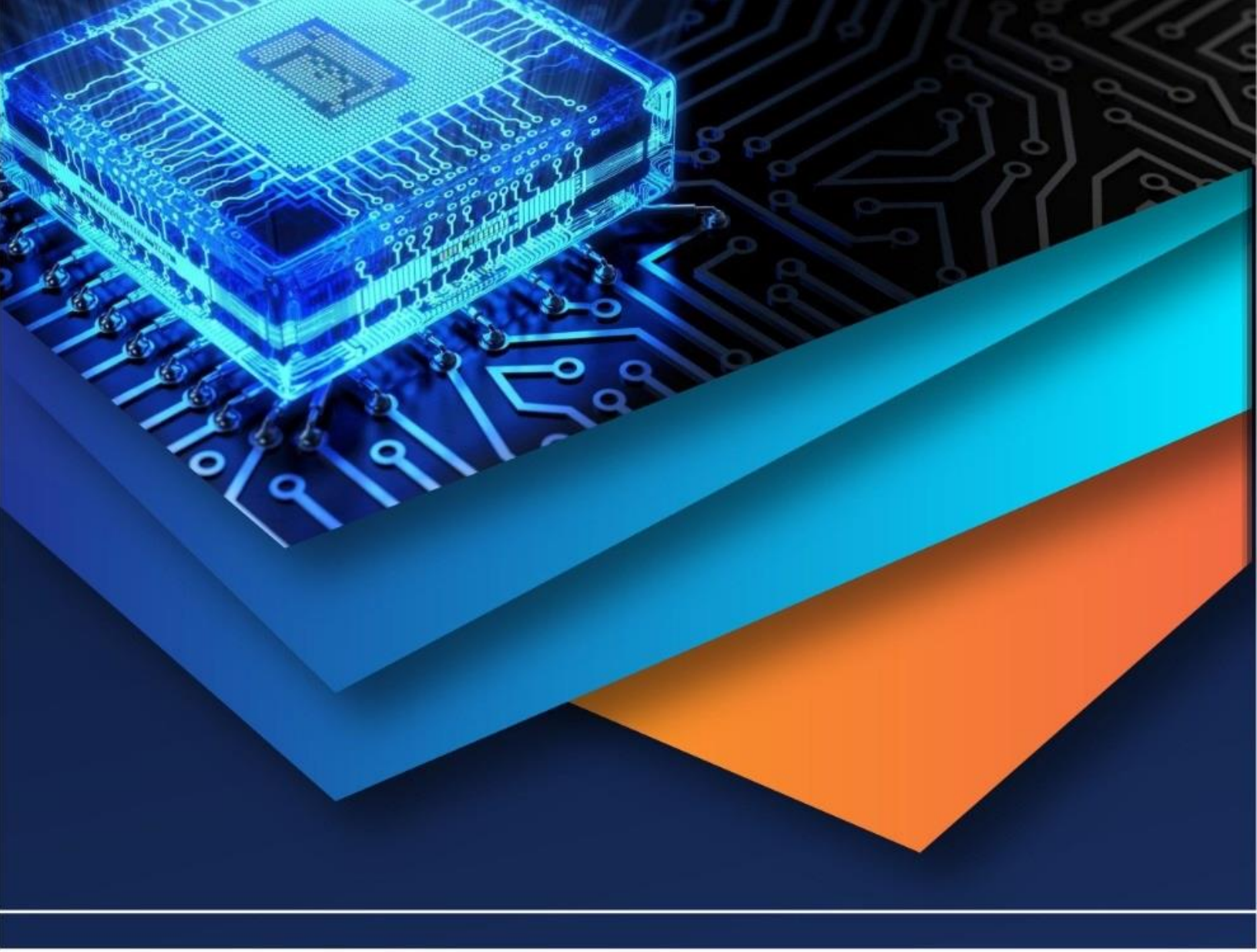
VII. CONCLUSION

In conclusion, hybrid algorithms offer a promising approach to enhancing fraud detection in the financial sector. By combining multiple techniques such as machine learning, deep learning, and ensemble methods, these models can leverage the strengths of different algorithms, resulting in improved accuracy and better handling of complex, imbalanced datasets. Deep learning models, such as neural networks, CNNs, and LSTMs, have shown significant potential in capturing intricate patterns in large datasets, often outperforming traditional models. Additionally, the integration of machine learning and deep learning methods enables models to continuously adapt and improve, leading to better detection and prevention of fraudulent activities. However, challenges such as data preprocessing, feature engineering, and evaluating model performance persist, emphasizing the importance of continuous research and development in this field. Ultimately, the use of hybrid algorithms in fraud detection holds great promise for improving financial security, reducing fraudulent activities, and optimizing operational efficiency in real-time transaction monitoring.

REFERENCES

[1] Pandey, K., Sachan, P., Ganpatrao, N.G., et al. (2021). A review of credit card fraud detection techniques. In Proceedings of the 2021 5th International Conference on Computing Methodologies and Communication (ICCMC) (pp. 1645–1653). IEEE.
[2] Lokanan, M.E. (2022). Financial fraud detection: The use of visualization techniques in credit card fraud and money laundering domains. Journal of Money Laundering Control, 26, 436–444.
[3] The Nilson Report. (2018). Global card fraud losses continue to rise.
[4] The Nilson Report. (2022). Global card fraud losses continue to rise.
[5] AARP. (2023). Identity fraud report. https://www.aarp.org/money/scams-fraud/info-2024/identity-fraud-report.html. Accessed: YYYY-MM-DD.
[6] Experian. (n.d.). Steps to take if you are the victim of credit card fraud. https://www.experian.com/blogs/ask-experian/steps-to-take-if-you-are-the-victim-of-credit-card-fraud/.
[7] Thennakoon, A., Bhagyani, C., Premadasa, S., Mihiranga, S., &Kuruwitaarachchi, N. (2019). Real-time credit card fraud detection using machine learning. In Proceedings of the 2019 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence) (pp. 488–493). IEEE.
[8] Kamusweke, K., Nyirenda, M., & Kabemba, M. (2019). Data mining for fraud detection in large scale financial transactions. EasyChair.
[9] Lim, K.S., Lee, L.H., & Sim, Y.W. (2021). A review of machine learning algorithms for fraud detection in credit card transactions. International Journal of Computer Science & Network Security, 21, 31–40.
[10] Barman, S., Pal, U., Sarfaraj, M.A., Biswas, B., Mahata, A., & Mandal, P. (2016). A complete literature review on financial fraud detection applying data mining techniques. International Journal of Trust Management in Computing and Communications, 3, 336–359.
[11] Padvekar, S.A., Kangane, P.M., & Jadhav, K.V. (2016). Credit card fraud detection system. International Journal of Engineering and Computer Science.
[12] Mathur, S., & Daniel, S. (2022). It's fraud! Application of machine learning techniques for detection of fraudulent digital advertising. Webology, 19, 2475–2490.
[13] Cortez, P., &Embrechts, M.J. (2013). Using sensitivity analysis and visualization techniques to open black box data mining models. Information Sciences, 225, 1–17.
[14] Maleki, F., Muthukrishnan, N., Ovens, K., Reinhold, C., & Forghani, R. (2020). Machine learning algorithm validation: From essentials to advanced applications and implications for regulatory certification and deployment. Neuroimaging Clinics, 30, 433–445.
[15] Orzechowski, P., &Boryczko, K. (2016). Hybrid biclustering algorithms for data mining. In Proceedings of the Applications of Evolutionary Computation: 19th European Conference, EvoApplications 2016 (pp. 156–168). Springer.
[16] Xie, Y., Li, A., Gao, L., & Liu, Z. (2021). A heterogeneous ensemble learning model based on data distribution for credit card fraud detection. Wireless Communications and Mobile Computing, 2021, 2531210.
[17] Kim, E., Lee, J., Shin, H., Yang, H., Cho, S., & Nam, S.K. (2021). [Additional reference information needed].
[18] Ouyang, X., & Wong, R. (2017). Credit card fraud detection using machine learning algorithms. Computers & Security, 68, 1–12.
[19] Li, J., Wang, Z., & Luo, W. (2020). A deep learning approach to credit card fraud detection. IEEE Transactions on Neural Networks and Learning Systems, 31, 4617–4630.
[20] Patil, S., & Mane, S. (2019). A comprehensive study of machine learning algorithms for fraud detection in credit card transactions. International Journal of Advanced Research in Computer Science, 10, 52–58.
[21] Zhang, T., Li, Z., & Yao, H. (2021). A hybrid machine learning model for fraud detection in financial transactions. Journal of Financial Technology, 8, 235–248.

[22] Gupta, M., & Agarwal, M. (2018). A review on data mining techniques for fraud detection in financial institutions. International Journal of Computer Applications, 180, 21–28.
[23] Bhattacharya, S., & Saha, S. (2020). Feature engineering for fraud detection: A review. International Journal of Computer Science and Information Security, 18, 98–103.
[24] Liu, Y., & Guo, Q. (2021). Machine learning techniques for real-time fraud detection: A survey. IEEE Access, 9, 12430–12442.
[25] Verma, A., & Sharma, R. (2019). Comparative analysis of machine learning algorithms for fraud detection. International Journal of Computer Applications, 182, 29–37.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY