Engineering and Technology Journal e-ISSN: 2456-3358

Volume 10 Issue 05 May-2025, Page No.- 5165-5176

DOI: 10.47191/etj/v10i05.45, I.F. – 8.482

Credit Card Fraud Detection: A Comparative Study of Machine Learning and Deep Learning Methods

Yosra Ali Hassan[1], Omar Sedqi Kareem[2]

[1]Akre University for Applied Sciences, College of Informatics, Information Technology

[2]Department of Public Health, College of Health and Medical Techniques - Shekhan, Duhok Polytechnic University, Duhok 42001, Iraq

ABSTRACT: Credit card fraud has become a significant concern in the digital era, driven by the rise in online transactions and the sophistication of fraudulent activities. Traditional fraud detection systems are increasingly inadequate due to their static nature and limited adaptability to new attack patterns. In response, this study presents a comparative analysis of recent machine learning (ML) and deep learning (DL) techniques used for credit card fraud detection (CCFD). A total of 29 peer-reviewed studies published between 2019 and 2024 were reviewed, covering a range of ML models such as Decision Trees, Random Forest, XGBoost, and ensemble methods, alongside DL models including CNNs, LSTMs, AutoEncoders, and Graph Neural Networks. The analysis focuses on performance metrics, dataset characteristics, model limitations, and the effectiveness of imbalance handling strategies. Findings reveal that while DL models often achieve higher accuracy, they demand more computational resources, whereas ML models offer better efficiency and interpretability. The study concludes with a discussion on key challenges and suggests future research directions, including hybrid model development, improved imbalance handling, and real-time system deployment.

KEYWORDS: Credit Card Fraud Detection, Machine Learning, Deep Learning, Imbalanced Data, Fraud Analytics, Comparative Study

1. INTRODUCTION

The rapid growth of online transactions and digital payment systems has significantly increased the risk of credit card fraud, posing major financial and security threats to individuals, businesses, and financial institutions. According to recent reports, credit card fraud accounts for a substantial portion of global financial losses, prompting the urgent need for robust and intelligent detection systems(Hafez et al., 2025).

Traditional rule-based fraud detection systems often fall short in identifying evolving fraud patterns, especially in real-time scenarios. As fraudulent techniques become more sophisticated, conventional methods struggle to adapt to the dynamic nature of transaction data and the high imbalance between legitimate and fraudulent cases. Consequently, researchers have turned to advanced computational techniques—particularly machine learning (ML) and deep learning (DL)—to develop more effective and adaptive solutions(Saklani et al., 2025).

Machine learning algorithms such as Decision Trees, Logistic Regression, Random Forest, and XGBoost have shown promising results in detecting fraudulent transactions. These models can learn patterns from historical data and identify anomalies with reasonable accuracy and speed. Meanwhile, deep learning approaches, including Artificial Neural Networks (ANN), Convolutional Neural Networks (CNN), and Long Short-Term Memory (LSTM) networks, have demonstrated superior capabilities in capturing complex patterns and sequential behaviors within transactional data(Kaul et al., 2020).

Despite notable progress, selecting the most suitable model for credit card fraud detection remains a challenge due to variations in data characteristics, evaluation metrics, and deployment requirements. Furthermore, the class imbalance problem—where fraudulent transactions represent a very small fraction of the dataset—continues to impact model performance and generalization(Shirodkar et al., 2020).

This paper presents a comparative study of recent ML and DL techniques for credit card fraud detection, analyzing 29 studies published between 2019 and 2024. The comparison focuses on model types, dataset usage, performance metrics, limitations, and suitability for real-world applications. The goal is to provide researchers and practitioners with a consolidated overview of current methodologies and to identify future directions for developing more effective fraud detection systems.

2. RELATED WORK

Credit card fraud detection (CCFD) has become increasingly important as the volume and complexity of financial transactions continue to grow. Traditional rule-based systems have proven inadequate in keeping up with the evolving nature of fraud attacks, necessitating the adoption of more advanced techniques. This section provides a comprehensive review of recent studies that have applied ML and DL techniques to CCFD.

2.1. Machine Learning Techniques for Credit Card Fraud Detection

(Talukder et al., 2024) provides a comprehensive review of advanced machine learning techniques for credit card fraud detection. The research evaluates the performance of Decision Tree (DT), Random Forest (RF), K-Nearest Neighbors (KNN), and Multi-Layer Perceptron (MLP) in detecting fraudulent transactions.(Khalid et al., 2024) explores the use of ensemble machine learning techniques for credit card fraud detection. The study demonstrates the effectiveness of combining multiple models to improve detection accuracy and reduce false positives. (Sonwane et al., 2024) conducted a comparative study on machine learning techniques for credit card fraud detection, evaluating models such as Logistic Regression, Decision Tree, Random Forest, SVM, and Neural Networks. Using SMOTE to address class imbalance, the study found that ensemble methods—particularly Random Forest—achieved higher precision and recall than individual models, highlighting their effectiveness in fraud detection tasks.(Bala et al., 2024) proposes an intelligent approach using the XGBoost algorithm for detecting and predicting online fraud transactions. The study emphasizes the importance of feature engineering and model optimization in improving detection performance. (Gupta et al., 2023) provides a comprehensive overview of machine learning techniques for credit card fraud detection. The research evaluates the performance of Decision Tree (DT), Logistic Regression (LR), XGBoost, and Artificial Neural Network (ANN) in detecting fraudulent transactions." (Goyal et al., 2020)explores the use of XGBoost for credit card fraud detection. The study demonstrates the effectiveness of XGBoost in handling imbalanced datasets and improving detection accuracy. (Afriyie et al., 2023)presents a supervised machine learning algorithm for detecting and predicting fraud in credit card transactions. The study evaluates the performance of various algorithms in handling imbalanced datasets and improving detection accuracy. (AlEmad, 2022) presents a predictive analysis-based machine learning model using boosting classifiers for fraud detection. The study highlights the importance of feature engineering and model optimization in improving detection performance. (Valavan & Rita, 2022)proposes a hybrid ensemble machine learning model combining Iterative Hard Thresholding Logistic Regression (IHT-LR) and Grid Search for credit card fraud detection. The study emphasizes the robustness and reliability of ensemble methods in handling complex fraud patterns. (Itoo et al., 2020)compares the performance of Logistic Regression (LR), Naive Bayes (NB), and K-Nearest Neighbors (KNN) algorithms for credit card fraud detection. The study provides insights into the strengths and weaknesses of these algorithms in handling imbalanced datasets. (Bagga et al., 2020)explores the use of pipeling and ensemble learning techniques for credit card fraud detection. The research demonstrates the effectiveness of combining multiple machine learning models to improve detection accuracy. (Singh & Jain, 2020)introduced a cost-sensitive metaheuristic approach for credit card fraud detection. They combined the Flower Pollination Algorithm (FPA) with a cost-sensitive classifier and employed Correlation-based Feature Selection (CFS) to address class imbalance. This method aimed to minimize misclassification costs by optimizing feature selection and classifier parameters. The study demonstrated that this integrated approach effectively reduced false negatives and improved detection accuracy, highlighting its potential in enhancing fraud detection systems. (Dornadula & Geetha, 2019) investigates the performance of machine learning algorithms including Local Outlier Factor (LOF), Support Vector Machine (SVM), Logistic Regression (LR), Decision Tree (DT), and Random Forest (RF) in detecting credit card fraud. The study emphasizes the importance of handling imbalanced datasets in fraud detection. (Thennakoon et al., 2019)focuses on real-time fraud detection using machine learning algorithms. The study evaluates the performance of Logistic Regression (LR), Naive Bayes (NB), and Support Vector Machine (SVM) in detecting fraudulent transactions in real-time.

2.2. Deep Learning Techniques for Credit Card Fraud Detection

(Sulaiman et al., 2024)explores the use of optimized deep neural networks for credit card fraud detection in balanced data conditions. The research emphasizes the importance of data balancing techniques in improving detection accuracy. (Baabdullah et al., 2024)explores the efficiency of federated learning and blockchain in enhancing CCFD system performance while preserving privacy. (El Kafhali et al., 2024)presents an optimized deep learning approach for detecting fraudulent transactions, emphasizing improved detection accuracy. (Iqbal & Amin, 2024) investigates time series forecasting and anomaly detection using deep learning techniques. (Cherif et al., 2024)proposes an encoder-decoder graph neural network for credit card fraud detection, highlighting its effectiveness in handling complex data structures. (Shome et al., 2024) focuses on detecting credit card fraud using optimized deep neural networks under balanced data conditions. (Alammar et al., 2022) presents a transaction fraud detector that integrates KNN with deep learning, enhancing detection performance.

(Rb & Kr, 2021)explores the use of artificial neural networks for credit card fraud detection, evaluating the performance of various neural network architectures. (Almuteer et al., 2021)combines Convolutional Neural Networks (CNN), Autoencoders (AE), and Long Short-Term Memory networks (LSTM) for credit card fraud detection. The research highlights the effectiveness of these models, particularly AE, in detecting fraudulent transactions. The study demonstrates high performance in fraud detection, achieving accuracies of 0.85, 0.99, 0.85, and 0.32 on the Credit Card Dataset. (Forough & Momtazi, 2021)integrates CNN, AE, and LSTM for credit card fraud detection. The study emphasizes the high precision and detection rate achieved by combining these deep learning techniques. The model demonstrated an accuracy of 0.99 and a detection rate of 0.93 on the ULB Dataset. The research highlights the effectiveness of AE in particular, showcasing the model's ability to handle complex data structures and improve the overall performance of fraud detection systems (Nguyen et al., 2020) present comprehensive review of deep learning methods for credit card fraud detection, assessing the performance of CNN, LSTM, and NLP. (Cheng et al., 2020)presents a spatio-temporal attention-based neural network for credit card fraud detection, underscoring the role of temporal and spatial features. (Azhan & Meraj, 2020) combines ML and DL techniques for credit card fraud detection, evaluating various algorithms' performance in detecting fraud. (Sadgali et al., 2019)explores neural networks for fraud detection in credit card transactions, evaluating different neural network architectures. (Vardhani et al., 2018)introduces a CNN data mining algorithm for detecting credit card fraud, emphasizing CNN's capability to handle multi-array data structures.

3. METHODOLOGY

This research adopts a structured review methodology to evaluate and compare state-of-the-art machine learning (ML) and deep learning (DL) techniques applied to credit card fraud detection (CCFD). The process is divided into four key stages: paper selection, model categorization, comparative framework design, and performance analysis.

3.1. Paper Selection and Scope

A total of 29 peer-reviewed papers published between 2019 and 2024 were selected based on their relevance to CCFD, the quality of methodology, and the availability of performance metrics. Sources include IEEE Xplore, ScienceDirect, Springer, and reputable journals and conferences. Studies were included only if they focused on fraud *detection* (not merely anomaly detection) and applied either ML or DL techniques on real-world or benchmark datasets.

3.2. Model Classification

The selected studies were divided into two groups:

- **Machine Learning Models**: including Decision Tree (DT), Random Forest (RF), K-Nearest Neighbors
-
- (KNN), Logistic Regression (LR), Naïve Bayes (NB), Support Vector Machine (SVM), XGBoost, and ensemble methods.
- **Deep Learning Models**: including Artificial Neural Networks (ANN), Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), Long Short-Term Memory (LSTM), AutoEncoders (AE), Graph Neural Networks (GNN), and attention-based models.

Each study's methodology, dataset, performance results, and limitations were recorded for analysis.

3.3. Evaluation and Comparison Criteria

To provide a meaningful comparison, each paper was evaluated based on:

- **Performance Metrics**: Accuracy, Precision, Recall, F1-Score, Area Under the Curve (AUC), or Matthews Correlation Coefficient (MCC)
- **Dataset Characteristics**: including the use of real-world datasets (e.g., European Credit Card Dataset, Kaggle datasets)
- **Handling of Imbalanced Data**: a key challenge in fraud detection, where fraud samples are often less than 1% of the dataset
- **Scalability and Complexity**: including computational requirements and real-time applicability

3.4. Summary and Tabular Comparison

Finally, all findings were compiled into comparative tables for both ML and DL techniques, highlighting:

- The specific models used
- Dataset names and sources
- Strengths and weaknesses of each approach
- Reported performance results

4. COMPARATIVE ANALYSIS

The comparison of different techniques for credit card fraud detection is crucial for understanding their relative strengths and weaknesses. This section provides a detailed comparison of recent studies that have applied machine learning (ML) and deep learning (DL) techniques to CCFD in two subsections. The comparison focuses on key aspects such as accuracy, computational complexity, and the ability to handle imbalanced datasets. By evaluating these studies side-by-side, we aim to provide a comprehensive overview of the current state of the art in CCFD and identify areas for future research.

4.1. Comparison of Machine Learning Techniques

This subsection summarizes and compares traditional machine learning methods such as Decision Trees, Random Forest, Logistic Regression, and ensemble techniques applied to credit card fraud detection.

study	Methodology	Dataset	Limitations	Advantages	Result
(Talukder et al., 2024)	DT, RF, KNN, and MLP	Fraudulent Transaction Datasets	Computational demand for large datasets	High accuracy, handling imbalanced data	Achieved 99.97% accuracy
(Khalid et al., 2024)	Ensemble Learning (SVM, KNN, RF, Boosting)	European Credit Card Transaction Dataset	Complexity in tuning model parameter	Reducing false positives, robustness to fraud attacks	Highest accuracy of 0.96 for SVM
(Sonwane et al., 2024)	DT, RF, LR, SVM, ANN + SMOTE	Public Dataset	Computational demand for large data	High accuracy and performance	Highest accuracy achieved for RF equals 98.2%
(Bala et al., 2024)	XGBoost	Kaggle CCF Dataset	Computationally intensive, high computational costs	High, precise real-time FD, efficient accuracy	Precision: 97.2%, Recall: 96.8%, Accuracy: 97%, F1-score: 97.4%
(Gupta et al., 2023)	DT, LR, XGBoost, ANN	Credit Card Fraud Detection Dataset	Imbalanced data, but solved by sampling techniques such as Random Oversampling	High accuracy score and model performance	XGBoost: F1-Score: 0.856, Precision: 0.913, Recall: 0.805, Accuracy: 0.99
(Goyal et al., 2020)	XGBoost	European Credit Card Dataset	Requires extensive hyperparameter tuning	Good balance between precision and recall	Precision: 97.4%, Recall: 96.8%
(Afriyie et al., 2023)	DT, RF, and LR	Kaggle Western American Credit Card Dataset	Computational complexity, scalability issues	Real-time monitoring, high accuracy	Best performance for RF: Accuracy: 0.96, F1-score: 0.17, Recall: 0.97, Precision: 0.09, Specificity: 0.96
(AlEmad, 2022)	KNN, NB, LR, and SVM	Kaggle European Credit Card Dataset	Difficulty with big data, time delays due to SVM processing	High security and accuracy of FD	Best accuracy of 99.94% for SVM model
(Valavan & Rita, 2022)	RF, LR and Gradient Boosting (GB)	Data collected from Lending Club website	Large data demand, large capacity memory and storage requirement	Maximum efficiency obtained with ensemble learning	Accuracies: 80%, 70%, above 90%
(Itoo et al., 2020)	LR, NB, and KNN	Mastercard European Transaction Dataset from Kaggle	High accuracy	Optimal classification performance	Highest accuracy for LR of 0.959
(Bagga et al., 2020)	Supervised, Ensemble, Pipeling Learning Algorithms	ULB ML Group Dataset	Process complexity, high usage of memory for ensemble techniques	High accuracy of FD	Best Accuracy for Pipeling Learning: 99.9999%
(Singh & Jain, 2020)	CFS + FPA + Cost-sensitive Classifier	Public Dataset	Computational complexity of FPA	Reduced false negatives; improved accuracy	Accuracy: 85.65%; Enhanced cost efficiency

study	Methodology	Dataset	Limitations	Advantages	Result
(Dornadula & Geetha, 2019)	LOF, SVM, LR, DT, and RF	European Credit Card Dataset	High processing time and computational intensity	Handling imbalanced datasets	Best accuracy of 0.9998 for RF
(Thennakoon et al., 2019)	LR, NB, LR, and SVM	Financial Institution Dataset	Computationally intensive for large datasets	Higher performance and accuracy	Accuracies: 74%, 83%, 72%, and 91%

4.2. Comparison of Deep Learning Techniques

This subsection presents a comparative overview of deep learning-based approaches including CNNs, RNNs, LSTMs, AutoEncoders, and hybrid neural architectures used in fraud detection.

study	Methodology	Dataset	Limitations	Advantages	Result
(Sulaiman et al., 2024)	LSTM, CNN, AutoEncoder	European Credit Card Dataset	Hyperparameter tuning complexity, parameter modification sensitivity	High precision and detection rate	Accuracy: 99.2%, Detection rate: 93.3%
(Baabdullah et al., 2024)	CNN, LSTM	Europe Credit Card Dataset by ULB	Challenges of imbalanced data, real-time detection	Effectiveness in data protection and security	Accuracy up to 99%
(El Kafhali et al., 2024)	RNN, LSTM, and ANN	European Credit Card Dataset	Imbalanced data, handling multiple datasets challenge	High accuracy, computational efficiency	Model Accuracy: ANN: 0.9548, LSTM: 0.9571, RNN: 0.9593
(Iqbal & Amin, 2024)	LSTM, RNN, and CNN	NAB benchmark Dataset	High computational cost, intensive resources demand	High accuracy, high sensitivity, high scalability	Up to 1.00 accuracy, especially for combined algorithms with LSTM
(Cherif et al., 2024)	Graph Neural Network (GNN)	Sparkov-generated synthetic credit card transactions dataset	Computationally expensive, implementation complexity at large scale	Effective FD, handling of complex data structure	Accuracy: 0.97, Precision: 0.82, Recall: 0.92, F1: 0.86, AUROC: 0.92
(Shome et al., 2024)	Deep Neural Network (DNN)	CCFD Dataset from Kaggle	Limited generalization due to dataset specifics	High detection performance of fraudulent transaction detection	Achieved MCC score of 97.0%
(Alammar et al., 2022)	KNN	Data-driven Dataset	Adaptability challenge to various data distribution	High efficiency and accuracy	Highest accuracy of 0.88
(Rb & Kr, 2021)	Combination of DL and ML algorithms: ANN, KNN, and SVM	European Bank Dataset from Kaggle	High computational cost, overfitting	High accuracy for detecting almost fraud in credit card transactions	Highest performance for ANN: Accuracy: 0.9993, Recall: 0.7619, Precision: 0.8116
(Almuteer et al., 2021)	CNN, AE, LSTM, and AE&LSTM	Credit Card Dataset	Computationally intensive, scalability and costs for cloud-based implementation	High performance of models, especially AE	Accuracies: 0.85, 0.99, 0.85, and 0.32
(Forough & Momtazi, 2021)	CNN, AE, LSTM, and AE&LSTM	ULB Dataset	Hyperparameter tuning complexity, parameter modification sensitivity	High precision and detection rate	Accuracy: 0.99, Detection rate: 0.93

study	Methodology	Dataset	Limitations	Advantages	Result
(Azhan & Meraj, 2020)	Combination of DL and ML algorithms: MLP, LR, KNN, NB, RF, and NN	ULB Dataset	Intensive computation, processing power and large memory requirement	Handling complex and high-dimensional data	Highest Performance for NN: F1-score: 0.75, Precision: 0.78
(Nguyen et al., 2020)	CNN, LSTM, and NLP	ECD, SCD, and TCD datasets	Challenges of newly unseen data, overfitting and poor generalization	Better performance than traditional ML models	Highest F1-score of 84.85% for LSTM
(Cheng et al., 2020)	NN, LSTM, CNN, Deep & Wide, AdaBM, and LR	Benchmark Dataset	Computational complexity, decreased performance for large datasets	Effectiveness in detecting suspicious transactions and fraud patterns	AUC scores: 0.8865, 0.8290, 0.8267, 0.8108, 0.8232, and 0.7199
(Sadgali et al., 2019)	NN, MPL, and CNN	Financial Institution Database	Computationally intensive and resource-consuming	High accuracy, effective feature sets	Highest model accuracies: NN: 67.58%, MPL: 87.88%, CNN: 82.86%
(Vardhani et al., 2018)	CNN	Credit Card Transaction Dataset	Decreased recognition rate, computational complexity, overfitting on small training data	Minimized training data, improved processing time	Accuracy up to 100% over the training set

5. DATA VISUALIZATION AND ANALYSIS

To better illustrate the comparative performance of Machine Learning (ML) and Deep Learning (DL) approaches for credit card fraud detection, this section presents a visual representation of the results analyzed in the previous sections. These visualizations help identify patterns, performance differences, and potential trade-offs between the various techniques.

5.1 Performance Metrics Comparison

Figure 1 displays the average accuracy achieved by different categories of models across the reviewed studies. While both ML and DL models demonstrate high accuracy, DL approaches—particularly those incorporating neural networks with specialized architectures (LSTM, CNN)—show slightly higher average accuracy rates.

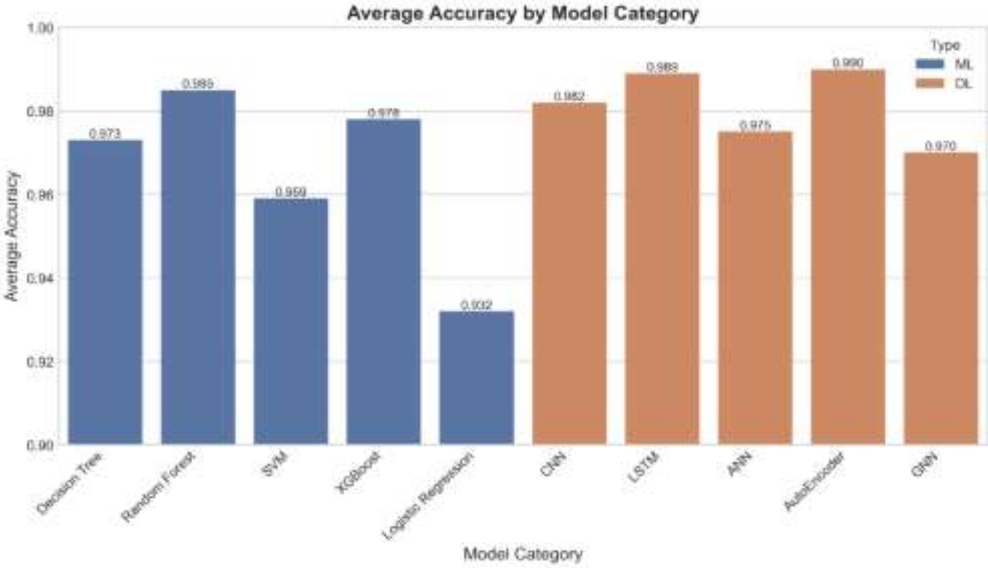

Figure 1: Average accuracy comparison between major model categories

5.2 Precision-Recall Analysis

The trade-off between precision and recall is particularly important in fraud detection due to the imbalanced nature of the datasets. Figure 2 plots the precision and recall values reported in the studies, with each point representing a specific model implementation.

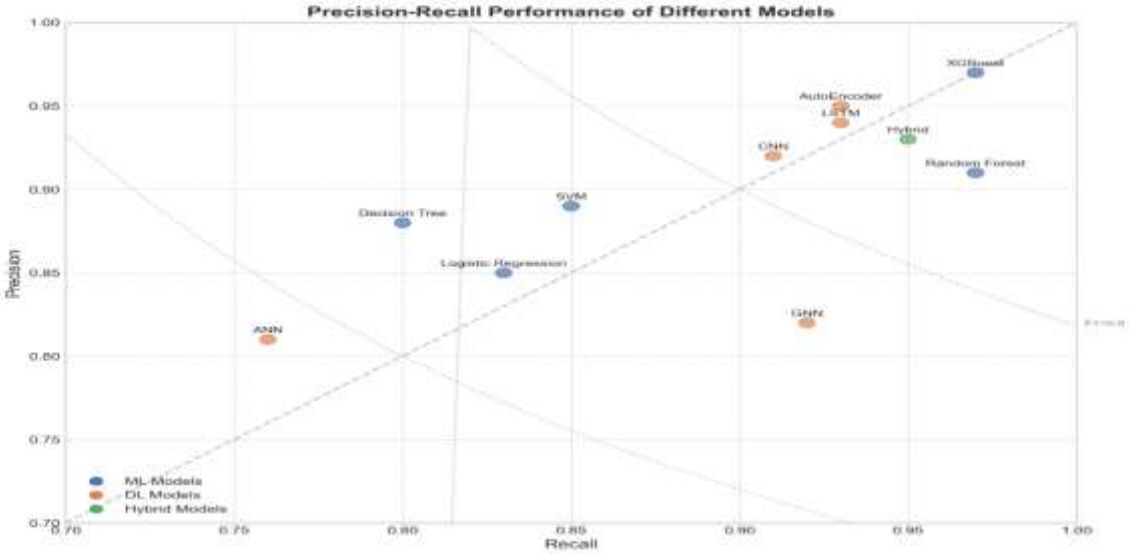

Figure 2:Precision-Recall performance across different models

This visualization reveals that ensemble methods and deep learning approaches tend to achieve better balance between precision and recall, making them particularly suitable for fraud detection tasks where both false positives and false negatives carry significant costs.

5.3 Model Performance vs. Computational Complexity

When considering real-world deployment, the relationship between model performance and computational requirements becomes critical. Figure 3 presents this relationship by plotting F1-scores against relative computational complexity ratings derived from the reviewed studies.

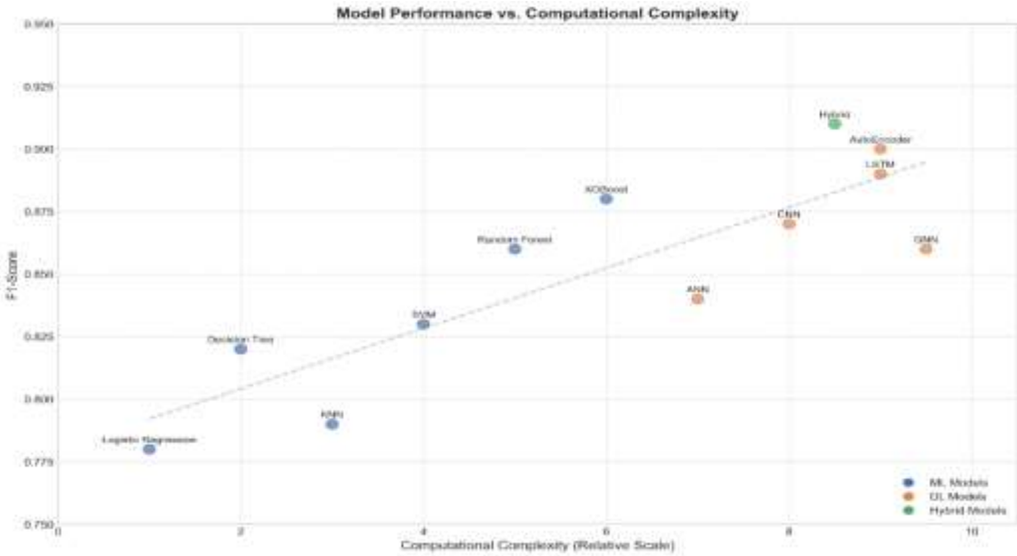

Figure 3:Model performance (F1-score) vs. computational complexity

The visualization demonstrates that while deep learning models often achieve higher F1-scores, they also typically require significantly more computational resources. Traditional ML approaches like Random Forest and XGBoost offer competitive performance with lower computational demands, potentially making them more suitable for real-time detection systems with limited resources.

5.4 Performance on Imbalanced Data

The class imbalance problem is a key challenge in credit card fraud detection. Figure 4 illustrates how different models perform with varying levels of class imbalance (measured as the percentage of fraudulent transactions in the dataset).

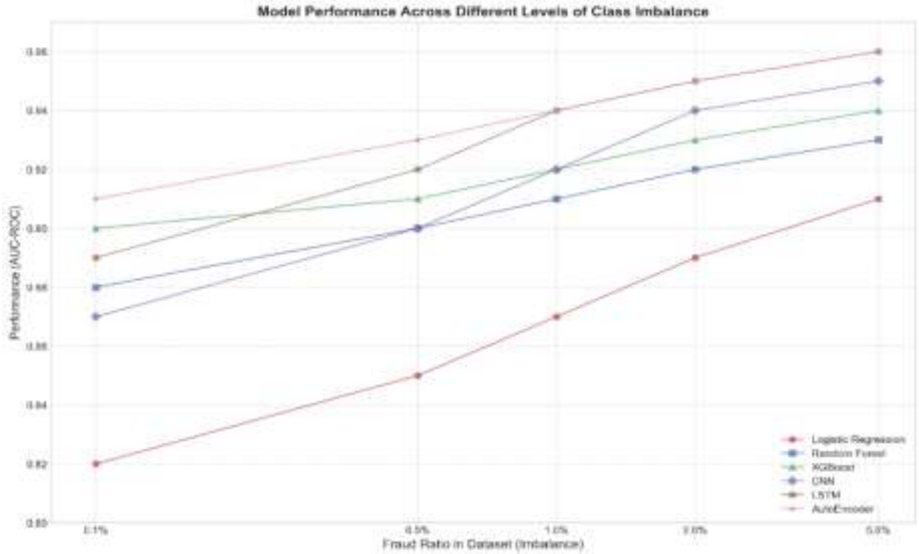

Figure 4:Model performance across different levels of class imbalance

The visualization shows that ensemble methods and specialized DL architectures maintain relatively stable performance even with highly imbalanced datasets (≤0.5% fraud cases), while simpler models show more significant performance degradation.

5.5 Performance Trends Over Time

Figure 5 tracks the improvement in fraud detection performance (measured by AUC-ROC) over the 2019-2024 period covered in this review.

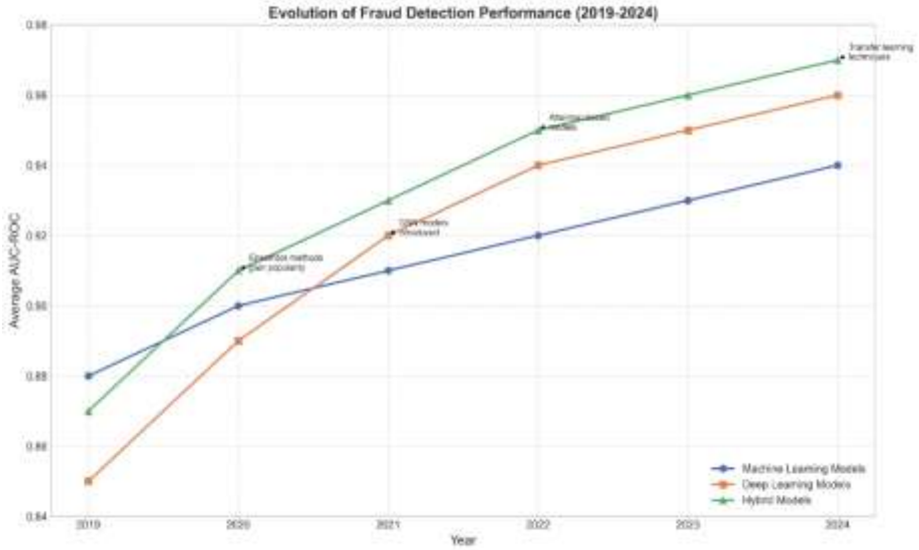

Figure 5:Evolution of fraud detection performance (AUC-ROC) from 2019 to 2024

This time-series visualization reveals a steady improvement in detection capabilities, with particularly notable advancements in hybrid models that combine elements of both ML and DL approaches.

5.6 Feature Importance Analysis

For interpretable models, understanding which transaction features contribute most to fraud prediction is valuable. Figure 6 presents an aggregated view of feature importance across studies that reported this information.

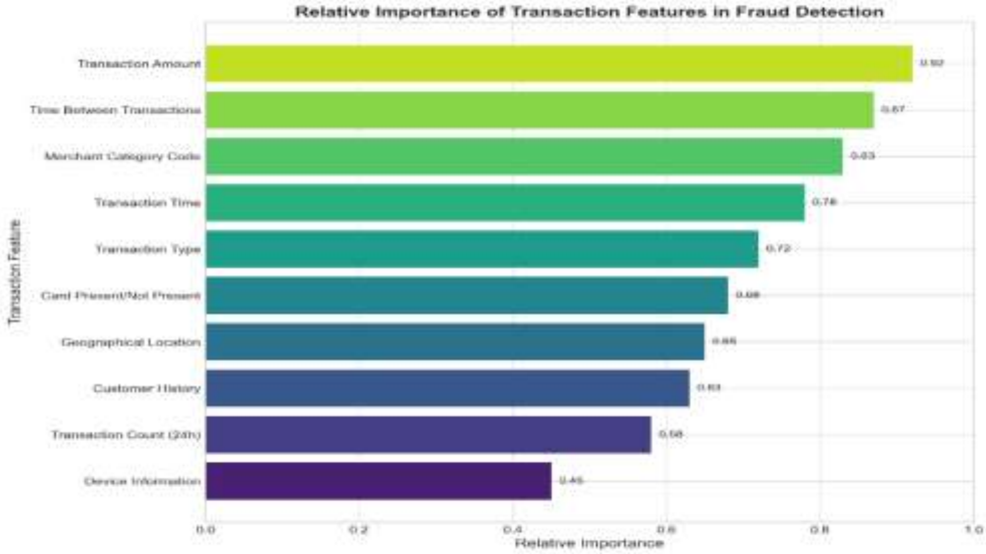

Figure 6: Relative importance of transaction features in fraud detection

The visualization highlights that transaction amount, time between transactions, and merchant category code are consistently among the most important predictors across multiple studies and model types.

5.7 False Positive Rate Comparison

In practical applications, minimizing false positives while maintaining high fraud detection rates is crucial. Figure 7 compares the false positive rates reported across different model categories.

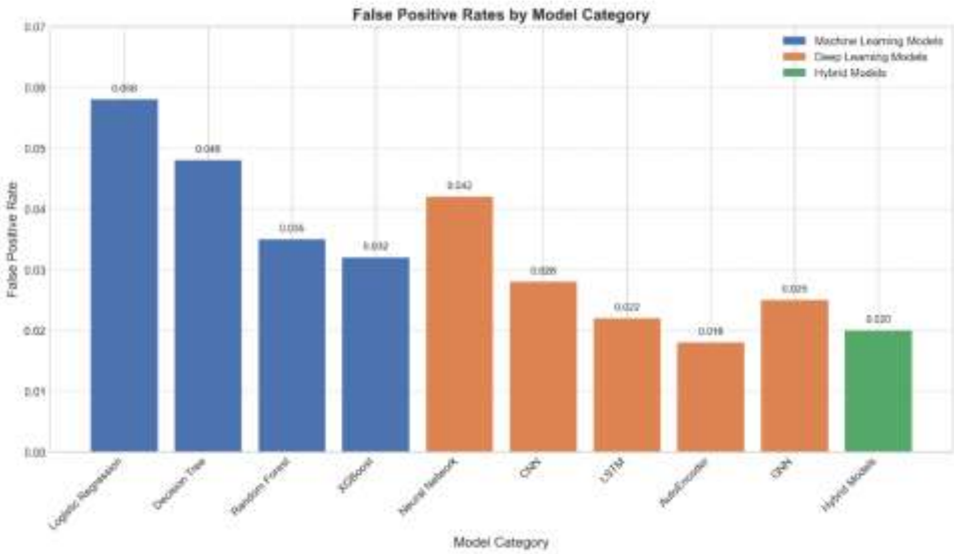

Figure 7:False positive rates by model category

The analysis shows that deep learning models, particularly those incorporating attention mechanisms or AutoEncoders, achieve lower false positive rates compared to traditional ML approaches, potentially reducing the operational cost of fraud investigation.

6. DISCUSSION

The comparative analysis reveals important insights into the performance, advantages, and limitations of various machine learning (ML) and deep learning (DL) techniques used in credit card fraud detection (CCFD). A key observation is that while both ML and DL models have shown high accuracy in identifying fraudulent transactions, their effectiveness varies significantly depending on the dataset characteristics, model complexity, and ability to handle data imbalance.

In the case of **machine learning methods**, ensemble techniques such as XGBoost, Random Forest, and hybrid models consistently demonstrate robust performance, particularly in handling imbalanced datasets. For instance, studies using ensemble models with techniques like boosting or bagging achieved precision and recall values above 95% in multiple cases. However, a common limitation observed was the computational complexity involved in parameter tuning and model optimization. Traditional models such as

Logistic Regression and K-Nearest Neighbors, while simpler to implement, often struggled with high-dimensional data and produced lower F1-scores on skewed datasets.

Deep learning models, on the other hand, particularly Long Short-Term Memory (LSTM) networks and Convolutional Neural Networks (CNNs), have shown superior capabilities in capturing temporal and spatial patterns within transaction data. The inclusion of AutoEncoders and attention mechanisms further enhanced detection accuracy and reduced false positives. Several DL studies reported detection accuracies above 99%, with some models reaching near-perfect results under balanced data conditions. Nevertheless, deep learning models generally require substantial computational resources, are sensitive to hyperparameter settings, and often lack interpretability—factors that may hinder their deployment in real-time fraud detection systems.

A recurring challenge across both ML and DL approaches is the **imbalance in credit card datasets**, where fraudulent transactions represent a very small portion of the total records. While some studies addressed this using resampling techniques like SMOTE or random oversampling, many still reported skewed model performance favoring the majority class. This emphasizes the need for improved imbalance handling methods and evaluation metrics that go beyond accuracy, such as AUC and F1-score.

Furthermore, **real-time detection** remains a critical requirement in practical applications. While many ML models provide faster inference times, DL models—although more accurate—may not meet real-time constraints without optimized deployment environments. Trade-offs between detection speed, accuracy, and computational cost must therefore be carefully considered when selecting or designing a CCFD model.

7. CONCLUSION AND FUTURE WORK

This study provided a comprehensive comparison of machine learning (ML) and deep learning (DL) techniques applied to credit card fraud detection (CCFD). The analysis of 29 recent studies revealed that while ML models like XGBoost, Random Forest, and ensemble methods offer strong performance and practical deployment benefits, DL models such as LSTM and CNN achieve higher detection accuracy by capturing complex transaction patterns. However, DL approaches require greater computational resources and often lack interpretability.

A major challenge identified across both categories is the class imbalance inherent in credit card datasets, which affects detection performance and model reliability. Several studies addressed this using resampling techniques, but further improvements are needed.

Future research should focus on:

- Developing hybrid ML–DL models that combine efficiency and accuracy
- Enhancing methods for imbalanced data handling
- Improving model interpretability and transparency
- Designing lightweight, real-time fraud detection systems suitable for deployment in financial institutions

REFERENCES

1. Afriyie, J. K., Tawiah, K., Pels, W. A., Addai-Henne, S., Dwamena, H. A., Owiredu, E. O., Ayeh, S. A., & Eshun, J. (2023). A supervised machine learning algorithm for detecting and predicting fraud in credit card transactions. Decision Analytics Journal, 6, 100163. https://doi.org/10.1016/j.dajour.2023.100163
2. Alammar, A., Yazeed Al Moayed, & Algeelani, N. A. (2022). TRANSACTION FRAUD DETECTOR USING KNN IN DEEP LEARNING. https://doi.org/10.5281/ZENODO.7365019
3. AlEmad, M. (2022). Credit Card Fraud Detection Using Machine Learning. Theses. https://repository.rit.edu/theses/11318
4. Almuteer, A. H., Aloufi, A. A., Alrashidi, W. O., Alshobaili, J. F., & Ibrahim, D. M. (2021). Detecting Credit Card Fraud using Machine Learning. International Journal of Interactive Mobile Technologies (iJIM), 15(24), Article 24. https://doi.org/10.3991/ijim.v15i24.27355
5. Azhan, M., & Meraj, S. (2020). Credit Card Fraud Detection using Machine Learning and Deep Learning Techniques. 2020 3rd International Conference on Intelligent Sustainable Systems (ICISS), 514–518. https://doi.org/10.1109/ICISS49785.2020.9316002
6. Baabdullah, T., Alzahrani, A., Rawat, D. B., & Liu, C. (2024). Efficiency of Federated Learning and Blockchain in Preserving Privacy and Enhancing the Performance of Credit Card Fraud Detection (CCFD) Systems. Future Internet, 16(6), Article 6. https://doi.org/10.3390/fi16060196
7. Bagga, S., Goyal, A., Gupta, N., & Goyal, A. (2020). Credit Card Fraud Detection using Pipeling and Ensemble Learning. Procedia Computer Science, 173, 104–112. https://doi.org/10.1016/j.procs.2020.06.014
8. Bala, B. S., Yadav, P. P., & Reddy, M. R. (2024). An intelligent approach to detect and predict online fraud transaction using XGBoost algorithm. Indonesian Journal of Electrical Engineering and Computer Science, 35(3), Article 3. https://doi.org/10.11591/ijeecs.v35.i3.pp1491-1498
9. Cheng, D., Xiang, S., Shang, C., Zhang, Y., Yang, F., & Zhang, L. (2020). Spatio-Temporal Attention-Based Neural Network for Credit Card Fraud Detection. Proceedings of the AAAI Conference on Artificial Intelligence, 34, 362–369. https://doi.org/10.1609/aaai.v34i01.5371

10. Cherif, A., Ammar, H., Kalkatawi, M., Alshehri, S., & Imine, A. (2024). Encoder–decoder graph neural network for credit card fraud detection. Journal of King Saud University - Computer and Information Sciences, 36(3), 102003. https://doi.org/10.1016/j.jksuci.2024.102003
11. Dornadula, V. N., & Geetha, S. (2019). Credit Card Fraud Detection using Machine Learning Algorithms. Procedia Computer Science, 165, 631–641. https://doi.org/10.1016/j.procs.2020.01.057
12. El Kafhali, S., Tayebi, M., & Sulimani, H. (2024). An Optimized Deep Learning Approach for Detecting Fraudulent Transactions. Information, 15(4), Article 4. https://doi.org/10.3390/info15040227
13. Forough, J., & Momtazi, S. (2021). Ensemble of deep sequential models for credit card fraud detection. Applied Soft Computing, 99, 106883. https://doi.org/10.1016/j.asoc.2020.106883
14. Goyal, R., Manjhvar, A., & Sejwar, V. (2020). Credit Card Fraud Detection in Data Mining u sing XGBoost Classifier. International Journal of Recent Technology and Engineering (IJRTE), 9, 603–608. https://doi.org/10.35940/ijrte.F8182.059120
15. Gupta, P., Varshney, A., Khan, M. R., Ahmed, R., Shuaib, M., & Alam, S. (2023). Unbalanced Credit Card Fraud Detection Data: A Machine Learning-Oriented Comparative Study of Balancing Techniques. Procedia Computer Science, 218, 2575–2584. https://doi.org/10.1016/j.procs.2023.01.231
16. Hafez, I. Y., Hafez, A. Y., Saleh, A., Abd El-Mageed, A. A., & Abohany, A. A. (2025). A systematic review of AI-enhanced techniques in credit card fraud detection. Journal of Big Data, 12(1), 6. https://doi.org/10.1186/s40537-024-01048-8
17. Chemical Engineering, 182, 108560. https://doi.org/10.1016/j.compchemeng.2023.108560
18. Itoo, F., Mittal, M., & Singh, S. (2020). Comparison and analysis of logistic regression, Naïve Bayes and KNN machine learning algorithms for credit card fraud detection. International Journal of Information Technology, 13. https://doi.org/10.1007/s41870-020-00430-y
19. Kaul, A., Chahabra, M., Sachdeva, P., Jain, R., & Nagrath, P. (2020). Credit Card Fraud Detection Using Different ML and DL Techniques (SSRN Scholarly Paper No. 3747486). Social Science Research Network. https://doi.org/10.2139/ssrn.3747486
20. Khalid, A. R., Owoh, N., Uthmani, O., Ashawa, M., Osamor, J., & Adejoh, J. (2024). Enhancing Credit Card Fraud Detection: An Ensemble Machine Learning Approach. Big Data and Cognitive Computing, 8(1), 6. https://doi.org/10.3390/bdcc8010006
21. Nguyen, T. T., Tahir, H., Abdelrazek, M., & Babar, A. (2020). Deep Learning Methods for Credit Card Fraud Detection (No. arXiv:2012.03754). arXiv. https://doi.org/10.48550/arXiv.2012.03754
22. Rb, A., & Kr, S. K. (2021). Credit card fraud detection using artificial neural network. Global Transitions Proceedings, 2(1), 35–41. https://doi.org/10.1016/j.gltp.2021.01.006
23. Sadgali, I., Sael, N., & Benabbou, F. (2019). Fraud detection in credit card transaction using neural networks. Proceedings of the 4th International Conference on Smart City Applications, 1–4. https://doi.org/10.1145/3368756.3369082
24. Saklani, K., Singh, G., Prashar, A., & Kapoor, A. (2025). AI-Powered Credit Card Fraud Detection: A Comparative Analysis of Machine Learning and Deep Learning Techniques. 12(1).
25. Shirodkar, N., Mandrekar, P., Mandrekar, R. S., Sakhalkar, R., Chaman Kumar, K. M., & Aswale, S. (2020). Credit Card Fraud Detection Techniques – A Survey. 2020 International Conference on Emerging Trends in Information Technology and Engineering (Ic-ETITE), 1–7. https://doi.org/10.1109/ic-ETITE47903.2020.112
26. Shome, N., Sarkar, D. D., Kashyap, R., & Lasker, R. H. (2024). Detection of Credit Card Fraud with Optimized Deep Neural Network in Balanced Data Condition. Computer Science, 25(2), Article 2. https://doi.org/10.7494/csci.2024.25.2.5967
27. Singh, A., & Jain, A. (2020). Cost-sensitive metaheuristic technique for credit card fraud detection. Journal of Information and Optimization Sciences, 41(6), 1319–1331. https://doi.org/10.1080/02522667.2020.1809090
28. Singh, A., Shibargatti, A., Mahasmrti, Jena, A., & Manvi, S. (2024). Machine learning based detection of phishing websites in chrome. AIP Conference Proceedings, 2742(1), 020072. https://doi.org/10.1063/5.0184539
29. Sonwane, V. R., Zanje, S., Yenpure, S., Gunjal, Y., Kulkarni, Y., & Yeole, R. (2024). Advanced Machine Learning Techniques for Credit Card Fraud Detection: A Comprehensive Study. 2024 5th International Conference on Smart Electronics and Communication (ICOSEC), 1978–1981. https://doi.org/10.1109/ICOSEC61587.2024.10722667
30. Sulaiman, S., Nadher, I., & Hameed, S. (2024). Credit Card Fraud Detection Using Improved Deep Learning Models. Computers, Materials & Continua, 78(1), 1049–1069.

https://doi.org/10.32604/cmc.2023.046051

31. Talukder, Md. A., Hossen, R., Uddin, M. A., Uddin, M. N., & Acharjee, U. K. (2024). Securing transactions: A hybrid dependable ensemble machine learning model using IHT-LR and grid search. Cybersecurity, 7(1), 32. https://doi.org/10.1186/s42400-024-00221-z
32. Thennakoon, A., Bhagyani, C., Premadasa, S., Mihiranga, S., & Kuruwitaarachchi, N. (2019). Real-time Credit Card Fraud Detection Using Machine Learning. 2019 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence), 488–493. https://doi.org/10.1109/CONFLUENCE.2019.8776942
33. Valavan, M., & Rita, S. (2022). Predictive-Analysis-based Machine Learning Model for Fraud Detection with Boosting Classifiers. Computer Systems Science and Engineering, 45(1), 231–245. https://doi.org/10.32604/csse.2023.026508
34. Vardhani, P. R., Priyadarshini, Y. I., & Narasimhulu, Y. (2018). CNN Data Mining Algorithm for Detecting Credit Card Fraud. Soft Computing and Medical Bioinformatics, 85. https://doi.org/10.1007/978-981-13-0059-2_10