Spectrum of Engineering Sciences
ISSN (e) 3007-3138 (p) 3007-312X Volume 4, Issue 5, 2026

COMPARATIVE ANALYSIS OF VARIOUS CREDIT CARD FRAUD DETECTION TECHNIQUES

Anam Irshad[*1], Khalid Hussain[2], Shoaib Ahmad Hashmi[3], Abrar Akram[4], Javaria Munir[5]

[*1,2,3,4,5]*Department of Computer Science & Information Technology, The Superior University Lahore, Pakistan*

[*1]anamirshad364@gmail.com, [2]khalidhussain.fsd@superior.edu.pk, [3]shoaibhashmi7860@gmail.com, [4]mabrar00269@gmail.com, [5]javariaasgharch358@gmail.com

DOI: https://doi.org/10.5281/zenodo.20391634

Keywords
Credit Card Fraud Detection, Machine Learning,Deep Learning, Imbalanced Datasets, Model Performance Evaluation, Naïve Bayes,Random Forest, Logistic Regression, KNN, CART, SVM, LDA, CNN, DNN, LSTM Ecommerce,Prediction, Classification, Bank

Article History
Received: 25 March 2026
Accepted: 04 May 2026
Published: 26 May 2026

Corresponding Author: *
Anam Irshad

Abstract
In the era of digital advancement, online transactions and digital payment system, credit cards are appearing as the biggest fraud. For improved banking security and reduce the financial threats, this fraud searching is occurring as the crucial element in this regard. This study is committed to have a look and draw comparison between various programs like Naïve Bayes, Random Forest, Logistic Regression,K-Nearest Neighbor,Classification and Regression Tree,Linear Discriminant Analysis,Deep Neural Network,Long Short Term Memory, Convolutional Neural Network and Support Vector Machine. Some tools are used to check the authenticity and precision of the models by testing and training. This may result the Deep Learning models and DNN proved to be the best and authentic models with the value 0. 9991.But in 2nd Dataset, the authenticity was achieved where DNN worked with the value 0.8166 in DL models which proved the best results. These results demonstrate that Deep Learning models perform well in the aspects like fraud searching and in complex transactions patterns. The findings of this research can assist researchers and financial institutions to choose appropriate fraud detection methods to create a secure online payment system process.

1.INTRODUCTION

The use of credit cards is becoming very common even in developing countries. People are now using credit cards for shopping and paying bills. But by increasing credit card users, fraud cases are also increasing day by day. Frauds related credit cards are causing loss of billions of dollars globally. We can define fraud as any act to deceive people for the sake of money. Frauds related to credit cards can be done by various means. It can be done by lost or stolen cards, by generating fake cards, by cloning the original sites, by altering the magnetic strip that is present on the card which has all the information of the user of that card and by stealing the data of the card's user from trading sites. Detection of fraud among thousands of genuine users is very challenging. As with advancement in fraudulent activities, it is very necessary to develop efficient methods to deal with these activities in their initial stages, so it doesn't reach the completion stage. Fraud detection deals with finding a fraud activity amongst thousands of genuine ones, which in fact puts forward a

challenge. Fraud detection means identifying fraudulent transactions from thousands of genuine transactions. This is a difficult task because fraudsters keep on develop new techniques. Therefore, it is important to create effective systems that can detect fraud at an early stage before major damage occurs. One major problem in fraud detection is that fraudulent transactions are less as compared to genuine transactions. Due to this, finding fraud accurately and efficiently becomes difficult. Credit card frauds can be of following types:

Application Frauds: It occurs when a fraudster gets the access to sensitive user information, such as usernames and passwords, and takes control of the application system to create a fake account. This type of fraud is usually linked to the theft of identity. In such cases, the fraudster applies for credit or a new credit card using the genuine cardholder's identity. They may also steal important documents to make their fraudulent application strong.

Electronic or Manual Credit Card Imprints: When the fraudster gains the information that is placed on the magnetic part of the card. The fraudulent can use this magnetic information in future to gain benefit from card.

CNP (Card Not Present): In this case the fraudulent need only the expiry date or the card number for transection through online method or on phone without having the card itself

Counterfeit Card Fraud: It is generally done when the fraudulent make the copy of the card it also happens when they have the information of the card. And these fake or copied card work like the real ones.

Lost and Stolen Card Fraud: In this cases when the original card holder lost their card or get stolen the fraudulent may use it for shopping through machine or online shopping because pin is usually not required in this cases.

Card ID Theft: This fraud resembles the application frauds. It occurs when criminals steal original cardholder information to use an already existing account or open a new account in the name of original cardholder. It is very difficult to detect.

The purpose of this study is to determine which strategy will be more effective in detecting credit card fraud by analyzing the benefits and drawbacks of both methods. Using a variety of evaluation metrics, the objective is to evaluate and compare the performance of different ML and DL models.

Research Objectives

- To compare the performance of DL and ML techniques for credit card fraud detection on imbalanced datasets using evaluation metrics such as accuracy, precision, recall, and F1-score.
- To evaluate and compare different ML and DL techniques for detecting credit card fraud.

Research Questions

- How do DL and ML techniques compare in performance for credit card fraud detection on imbalanced datasets?
- Which DL and ML techniques provide highest accuracy for identifying credit card scam?

2. Literature Review

Card fraud is becoming a topic of study due to the quick expansion of internet services like online banking, online payments, and e-commerce. Many researchers have used DL and ML to address financial fraud and loss detection. Several ML techniques, such as Support Vector Machine (SVM), Artificial Neural Network (ANN), Decision Tree (DT), K-Nearest Neighbor (KNN), and Bayesian Network, have been used to try and detect fraud [1]. According to the study, ANN was able to achieve high accuracy, but false alarms and the inability to identify novel fraud patterns persisted. Additionally, Lakshmi and Kavila tested the Random Forest (RF), Decision Tree (DT), and Logistic Regression (LR) models. They discovered that the Random Forest model performed best when trained on the unbalanced data [2]. However, time-based approaches that could help identify new fraud trends were not used in their research. The ensemble learning approach is frequently used to identify fraud and is made up of several models to produce better results. In order to detect fraud, Dhankhad et al. employed

supervised and ensemble ML techniques. They found that using these methods would result in a higher prediction accuracy [3]. However, they discovered that some data sets in the study were not balanced. Similarly, an XGBoost-based fraud detection model that outperformed fraud detection on unbalanced datasets was presented by Do et al. [4]. There were many false alarms for the typical times, despite the model's reasonable quality. Because deep learning can automatically extract intricate patterns from transaction data, it has gained popularity in recent years. Nguyen et al. suggested a method based on CNN and LSTM models to detect credit card fraud and showed that deep learning models outperform conventional ML models [5]. However, when the data set is unbalanced or the models are tested against data they have never seen, their performance would decline. In a different study, Alarfaj et al. used CNN models and discovered that they were highly accurate in detecting fraud; however, they also suggested that there might be problems with their implementation and that they might produce false negative rates [6]. Some researchers focused on using models of the Multilayer Perceptron (MLP) type to detect fraud. In order to improve the accuracy of fraud detection, Kasasbeh et al. proposed an ANN model using different evaluation functions, which is improved by using an MLP-based ANN model [7]. MLP outperformed Extreme Learning Machine (ELM) models in classification, according to El Hlouli et al.'s comparison [8]. Similarly, El Naby et al. achieved high fraud detection performance by combining CNN and MLP models and using oversampling techniques [9]. The majority of earlier research was successful in achieving high accuracy, but these studies all used balanced datasets or single models. A real-time unbalanced dataset with a high percentage of fraudulent transactions relative to regular transactions was not taken into account by the majority of the research. Some of the studies also mentioned high false positive rates and a lack of flexibility in response to shifting fraud patterns. As a result, comparative research on unbalanced datasets that characterizes performance using F1-score, accuracy, precision, and recall has not yet been done on ML and DL techniques.

3.Methodology

Dataset Description

Three well-known benchmark datasets are used in this study to train and evaluate each model. 31 attributes and 248,516 transactions make up the first data set, which describes a range of characteristics. 52,125 transactions and 29 features make up the second dataset, which combines numerical and categorical data.

Proposed Framework

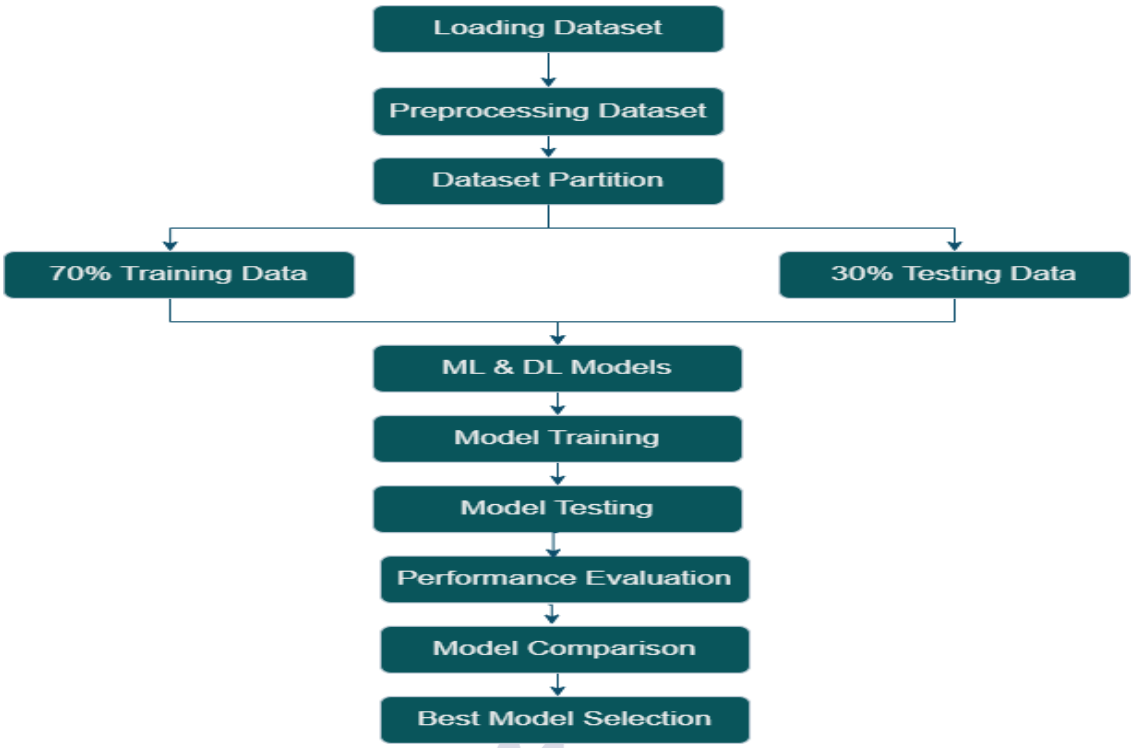

***Figure 1*: Credit Card Fraud Detection Architectural Diagram**

Figure 1 provides an explanation of a thorough fraud detection procedure. after the Kaggle dataset has been imported. Next, pre-process the data set to eliminate any dirty data, which may include missing values. Data is separated into training and testing data sets after being cleaned. The data distribution ratio of 0.70 (70%) training data and 0.3 (30%) testing data. Training data is used to train all ML models and DL models. Once the data has been "trained," the testing dataset is used to test the models. The best model for detecting credit card fraud is then determined by evaluating each model based on its accuracy score, precession score, recall, true positive,true negative, and confusion matrix. After models training and testing results of all ten models are compared. The following models are trained and tested.

i. Naive Bayes
ii. Random Forest
iii. Logistic Regression
iv. K-Nearest Neighbor
v. Classification & Regression Tree
vi. Linear Discriminant Analysis
vii. Deep Neural Network
viii. Convolutional Neural Network
ix. Long-Short Term Memory
x. Support Vector Machine

4.Results and Discussion

Results of Dataset-1

Table 1: Performance comparison of ML and DL models

Sr. No	Model Name	Training Accuracy	Testing Accuracy	Precision	Recall	F1_Score
1	Naïve Bayes	0.9780	0.9518	0.5300	0.8950	0.5500
2	Random Forest	1.0000	0.9235	0.9750	0.8700	0.9150
3	Logistic Regression	0.9993	0.9689	0.9250	0.8600	0.8900
4	KNN (K-Nearest Neighbor)	0.9995	0.9052	0.9750	0.8500	0.9050
5	CART (Classification & Regression Tree)	0.9994	0.9518	0.9250	0.8400	0.8750
6	LDA (Linear Discriminant Analysis)	0.9994	0.9048	0.9250	0.8450	0.8950
7	DNN (Deep Neural Network)	0.9999	0.9991	0.9248	0.8444	0.8946
8	CNN (Convolution Neural Network)	0.9997	0.9950	0.9248	0.8444	0.8946
9	LSTM (Long-Short Term Memory)	0.9982	0.9981	0.9248	0.8444	0.8946
10	SVM (Support Vector Machine)	0.9997	0.9518	0.9800	0.7950	0.8650

The given table shows “Logistic Regression” with 0.9689 accuracy performing well from ML models, while in DL models DNN is performing well with accuracy 0.9991 which is considered as best accuracy.

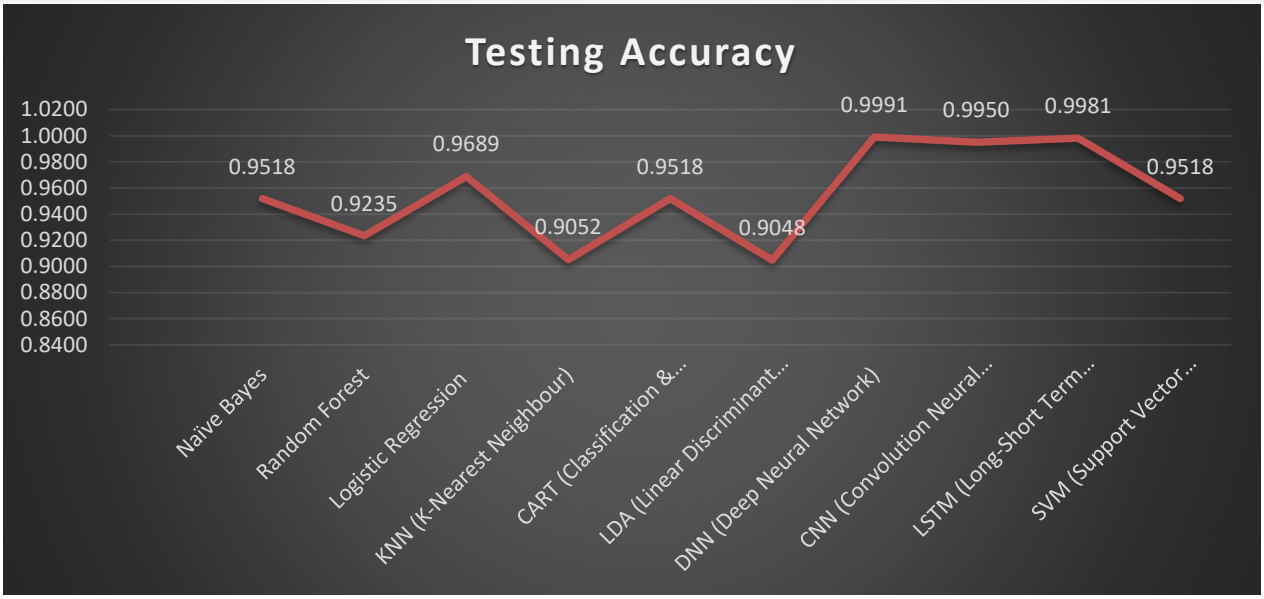

Figure 2. Graph of Dataset-1 models based on 70% Training and 30% Testing Split Ratio

Results of Dataset-2

Table 2:Comparison of ML and DL models

Sr. No	Model Name	Training Accuracy	Testing Accuracy	Precision	Recall	F1_Score
1	Naïve Bayes	0.3796	0.3598	0.5550	0.5550	0.3600
2	Random Forest	1.0000	0.7624	0.7350	0.6600	0.7250
3	Logistic Regression	0.7755	0.6351	0.3950	0.5000	0.4400
4	KNN(K-Nearest Neighbor)	0.8005	0.6136	0.6000	0.5500	0.5550
5	CART (Classification & Regression Tree)	0.8217	0.6628	0.7400	0.6600	0.6850
6	LDA(Linear Discriminant Analysis)	0.3796	0.3598	0.7500	0.6200	0.6400
7	DNN (Deep Neural Network)	0.8208	0.8166	0.7548	0.5848	0.6287
8	CNN (Convolution Neural Network)	0.8448	0.8133	0.7548	0.5848	0.6287

9	LSTM (Long-Short Term Memory)	0.7747	0.7920	0.7548	0.5848	0.6287
10	SVM (Support Vector Machine)	0.7757	0.6628	0.3950	0.5000	0.4400

The given table shows "Random Forest" with 0.7624 accuracy performing well from ML models, while in DL models DNN is performing well with accuracy 0.8166 which is considered as best accuracy.

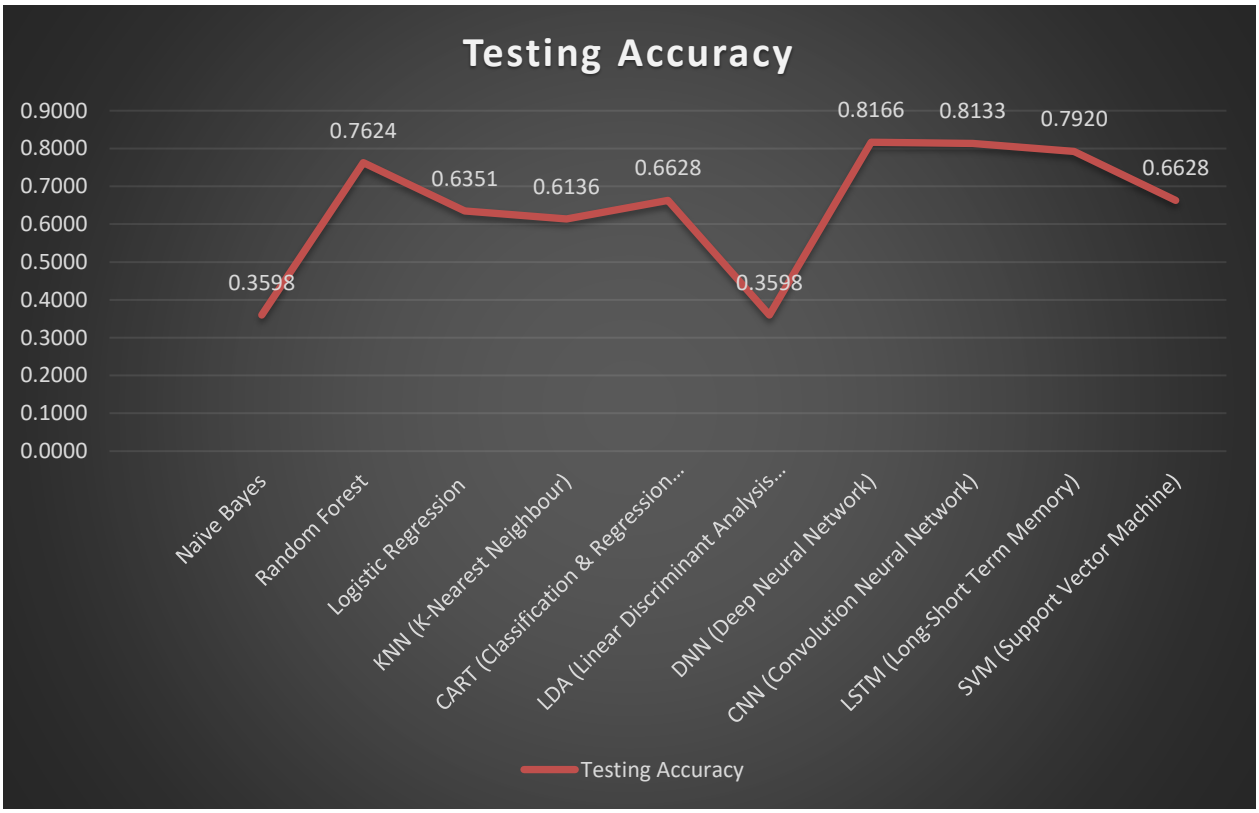

Figure 3. Graph of Dataset-2 models based on 70% Training and 30% Testing Split Ratio

5.Conclusion

This study explains and compares the various ML and DL techniques in relation to identifying Credit Card Fraud. Ten models, including NB, RF, LR, KNN, CART, LDA, DNN, CNN, LSTM, and SVM, were trained and tested on two distinct datasets. The models' performance was assessed using F1-score, recall, accuracy, and precision. It is evident from the experimental findings that the suggested models produced by deep learning outperformed those produced by conventional ML. With a test accuracy of 0.9689, Logistic Regression was the best-performing ML model for Dataset-1, while the DNN model had the highest accuracy of 0.9991. Similarly, among all ML models in Dataset-2, the Random Forest model achieved the highest accuracy of 0.7624, while the DNN model achieved the highest accuracy of 0.8166. According to the study, DL is now more successful in identifying increasingly intricate fraud patterns in credit card transactions. Additionally, there were a few low-complexity ML models with excellent performance. The findings demonstrated that the characteristics of the data

set and the intended performance goal determine which model should be used for fraud detection. In addition to real-time fraud detection systems and the application of more sophisticated deep learning techniques to detect fraud, future research may examine hybrid models for increasing fraud detection accuracy while decreasing false alarms.

REFERENCES

[1] Y. Jain, N. Tiwari, S. Dubey, and S. Jain, "A comparative analysis of various credit card fraud detection techniques," International Journal of Recent Technology and Engineering, vol. 7, no. 5, 2019.

[2] L. S. V S S and S. Deepthi Kavila, "Machine Learning For Credit Card Fraud Detection System," 2018. [Online]. Available: http://www.ripublication.com

[3] S. Dhankhad, E. A. Mohammed, and B. Far, "Supervised machine learning algorithms for credit card fraudulent transaction detection: A comparative study," in Proceedings - 2018 IEEE 19th International Conference on Information Reuse and Integration for Data Science, IRI 2018, 2018. doi: 10.1109/IRI.2018.00025.

[4] C. Do Xuan, D. Ngoc Phong, and N. Duy Phuong, "A new approach for detecting credit card fraud transaction," International Journal of Nonlinear Analysis and Applications, vol. 14, no. 5, 2023.

[5] M. A. Alrasheedi, "Enhancing Fraud Detection in Credit Card Transactions: A Comparative Study of Machine Learning Models," Comput. Econ., 2025, doi: 10.1007/s10614-025-11071-3.

[6] F. K. Alarfaj, I. Malik, H. U. Khan, N. Almusallam, M. Ramzan, and M. Ahmed, "Credit Card Fraud Detection Using State-of-the-Art Machine Learning and Deep Learning Algorithms," IEEE Access, vol. 10, 2022, doi: 10.1109/ACCESS.2022.3166891.

[7] B. Kasasbeh, B. Aldabaybah, and H. Ahmad, "Multilayer perceptron artificial neural networks-based model for credit card fraud detection," Indonesian Journal of Electrical Engineering and Computer Science, vol. 26, no. 1, 2022, doi: 10.11591/ijeecs.v26.i1.pp362-373.

[8] F. Z. El Hlouli, J. Riffi, M. A. Mahraz, A. El Yahyaouy, and H. Tairi, "Credit Card Fraud Detection Based on Multilayer Perceptron and Extreme Learning Machine Architectures," in 2020 International Conference on Intelligent Systems and Computer Vision, ISCV 2020, 2020. doi: 10.1109/ISCV49265.2020.9204185.

[9] A. A. El Naby, E. El-Din Hemdan, and A. El-Sayed, "Deep learning approach for credit card fraud detection," in ICEEM 2021 - 2nd IEEE International Conference on Electronic Engineering, 2021. doi: 10.1109/ICEEM52022.2021.9480639.