CREDIT CARD FRAUD DETECTION USING ML

A PROJECT REPORT

SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE AWARD OF THE DEGREE
OF

MASTER OF TECHNOLOGY
IN
INFORMATION TECHNOLOGY

SUBMITTED BY:
ASHA KUMARI (2K23/ITY/25)

Under the supervision of
DR. ANAMIKA CHAUHAN

DEPARTMENT OF INFORMATION TECHNOLOGY
DELHI TECHNOLOGICAL UNIVERSITY
(Formerly, Delhi College of Engineering) Bawana Road, Delhi-110042

MAY, 2025

CANDIDATE'S DECLARATION

I, **Asha Kumari, 2K23/ITY/25** student of M. Tech., Information Technology, hereby declares that the project Dissertation titled "**Credit Card Fraud Detection Using ML**" which is submitted by me to the Department of Information Technology, Delhi Technological University, Delhi in partial fulfillment of the requirement for the award of the degree of Master of Technology is original and not copied from any source without proper citation. This work has not previously formed the basis for the award of any Degree, Diploma Associateship, Fellowship, or other similar title or recognition.

Place: **Delhi**	**Asha Kumari**
Date: 29th May 2025	**(2K23/ITY/25)**

DEPARTMENT OF INFORMATION TECHNOLOGY
DELHI TECHNOLOGICAL UNIVERSITY
(Formerly, Delhi College of Engineering)
Bawana Road, Delhi-110042

CERTIFICATE

I hereby certify that the Project Dissertation titled "**Credit Card Fraud Detection Using ML**" which is submitted by **Asha Kumari**, **2K23/ITY/25** from the Department of **Information Technology**, **Delhi Technological University**, Delhi in partial fulfillment of the requirement for the award of the Degree of Master of Technology, is a record of the project work carried out by the students under my supervision. To the best of my knowledge, this work has not been submitted in part or full for any Degree or Diploma to this University or elsewhere.

Place: Delhi
Date: 29th May 2025

DR. ANAMIKA CHAUHAN
SUPERVISOR
(Assistant Professor)
Dept. of Information Technology

ABSTRACT

This thesis investigates the potency of supervised machine learning techniques for detecting credit card fraud in highly imbalanced transaction data. Using a publicly available dataset of over 1.6 million transactions only 0.5% of which are fraudulent five approaches (Random Forest, Decision Tree, Naive Bayes, Logistic Regression, and LSTM) were carried out and evaluated on a 70:30 train–test split. To confront the hurdle of skewed class ratio, the Synthetic Minority Over-sampling Technique (SMOTE) was employed in coordination with Random Forest and LSTM, generating realistic synthetic fraud instances. Model performance was assessed via confusion matrices and assessment criterion accuracy, precision, sensitivity, F1-score, and ROC-AUC alongside computational efficiency. On the original imbalanced data, Random Forest achieved the highest accuracy (99.77%) but exhibited low recall, indicating many missed fraud cases. After SMOTE, all models showed marked improvement in recall and F1-score, with LSTM outperforming others (99.87% accuracy, 93.73% recall, 92.85% F1-score, 99.75% ROC-AUC). These findings demonstrate that combining deep learning with targeted oversampling yields the most balanced fraud detection performance. The study offers feasible guidance targeted at financial entities pursuing adaptive, data-driven fraud prevention solutions and arranges the groundwork for future research into real-time and hybrid detection systems.

ACKNOWLEDGEMENT

We would like to express our heartfelt gratitude to all the individuals who have supported and assisted us throughout our M. Tech Major Project. First and foremost, we would like to thank our project supervisor, "**Dr. Anamika Chauhan"**, *Assistant Professor*, Department of Information Technology, Delhi Technological University for his constant guidance, support, and encouragement throughout the project. We are indebted to him for sharing his knowledge, expertise, and valuable feedback that helped us in shaping the project.

We are also thankful to our parents for their constant support and motivation, which has been our driving force throughout our academic pursuits. We would like to express our gratitude to our friends and classmates who have been a constant source of inspiration and motivation.

Asha Kumari

(2K23/ITY/25)

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

1.1 Context

In the modern era, credit cards are widely used for shopping, paying bills, and making online purchases. While they offer great convenience, they also come with risks especially the risk of fraud. Credit card fraud takes place when unauthorized person uses your card or its details without your consent to make purchases or withdraw funds.

With the increased use of digital transactions and web shopping, criminals have discovered new ways to steal credit card details. The most common methods include website hacking, tricking people into divulging their card numbers, or utilizing devices to scan data from physical cards. Therefore, credit card fraud has become an apprehension to card issuers, card providers, and consumers alike. To counter this menace, companies have fraud detection systems that track activity on transactions.

These systems function like virtual security watchmen, scanning every transaction for possible indicators of suspicious activity. For example, if an unexpected high value transaction is made in a foreign country or if a pattern of transactions looks suspicious, the system can report the incident to the authorities by flagging the activity.

Current fraud detection equipment has continued to become more sophisticated, particularly with the inclusion of machine learning. Such technology allows systems to learn from past transaction history and identify patterns of behavior, which will help distinguish between normal activity and suspicious activity. For instance, if an individual usually does local shopping and a sudden big purchase is made overseas, the system might flag that as unusual behavior. Essentially, credit card fraud detection is based on cutting edge technology to protect user's money and step in before fraud can occur.

1.2 Background

The quick growth of new ways of paying electronically online buying, mobile phone payment apps, and contactless payments has greatly changed how individuals carry money and spend it. Credit cards, however, are still a popular and convenient means of payment. Yet at the same time, the convenience of their usage makes them also susceptible to abuse. Over the last few years, credit card fraud has skyrocketed, with international financial losses rising significantly from an estimated $16 billion in 2015 to an anticipated $43 billion by 2026 (see Fig. 1). This dramatic rise is indicative of increased sophistication on the part of fraudsters and the greater challenge of blocking it.

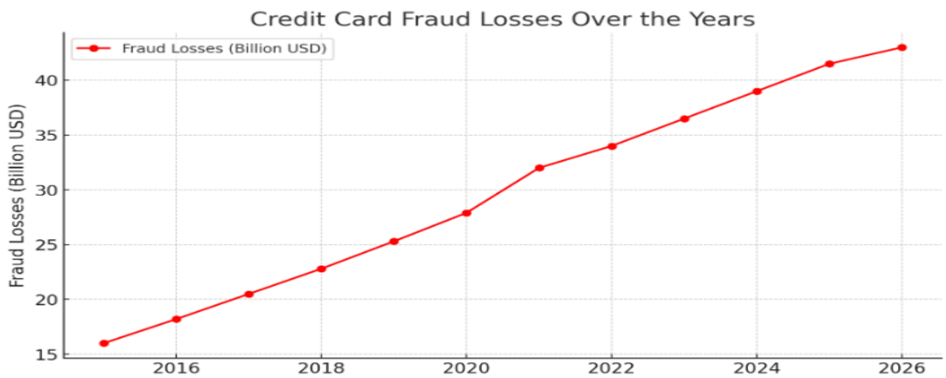


Fig.1.1 Number of Credit Card Fraud losses over Times

As the level and sophistication of digital transactions rise, cyber criminals are continually devising new means of taking advantage of system vulnerabilities as well as user behavior. Conventional techniques in fraud detection, namely guideline founded on systems and visual verify, are no longer powerful to detect the changing modus operandi of fraudsters. Data mining has thus emerged as a leading method for detecting fraud. It entails searching large collections of transactional records to uncover concealed patterns, detect abnormal behavior, and label transactions as either authentic or fraudulent. This activity assists financial system to respond quickly to possible threats.

In recent advancements, sophisticated methods among which is Long Short-Term Memory (LSTM) networks have found popularity for their performance in analyzing sequences of information. Dissimilar to conventional models, LSTM – a method under deep learning – has the capability to learn time- based relationships within transaction histories and respond to changing patterns of fraudulent activities. This makes them especially appropriate for real-time fraud detection. When coupled with robust data preparation methods and class balancing methods like SMOTE, these models form a solid foundation for current fraud detection frameworks.

1.3 Motivation

Fraud detection using credit card data is a tough responsibility owing to the data from transactions is extremely skewed in nature – with loads of genuine transactions far outnumbering fraud transactions. Such an imbalance makes it difficult for typical detection mechanisms to spot suspicious activity from genuine activity with accuracy. An extremely risk- averse system will mistakenly alert legitimate transactions (false positives), which will inconvenience customers, while a less strict one could miss suspicious transactions (false negatives), resulting in economic damages. Finding the right balance between these extremes is both essential and challenging.

The challenge is further compounded by the fact that fraudsters continually evolve their tactics. They adapt rapidly to security technologies, constantly developing new methods of evading protective measures. Older fraud detection methods thus can become obsolete and less effective. It is therefore necessary for detection systems to be intelligent, adaptive, and able to learn from upcoming patterns and changing data.

To address such challenges, the current research investigates the application of ensemble machine learning models of different strength in pattern detection and data classification. It also employs the Synthetic Minority Oversampling Technique (SMOTE) to tackle unequal class distribution issue through the creation of synthetic samples of fraudulent transactions. This enables the models to better identify rare fraudulent activity without overestimating the large volume of legitimate transactions.

The prime concentrate of this thesis is to analyze and evaluate the capability of distinct machine learning approaches- Random Forest, Decision Tree, Naïve Bayes, Logistic Regression, and Long Short-Term Memory (LSTM) both with and without using SMOTE. The purpose is to find those methods that best identify fraud transactions while keeping false positives low.

Ultimately, this study contributes to enhancing the security and dependability of financial systems, supporting safer use of credit cards in an increasingly digital world.

1.4 Problem Statement

Distinguishing credit card fraud is a challenging process because the highly skewed distribution of transaction datasets, with the fraud being a minor fraction of legitimate transactions, tends to reason machine learning algorithms to lean inclined to the majority class. Therefore, fraudulent activities can easily go undetected, while legitimate transactions would be falsely identified as fraud, causing dissatisfaction among customers and posing financial risks to institutions.

Besides the imbalance in data, fraud activity is dynamic and evolving in nature. This dynamism renders conventional detection strategies ineffective since they struggle to keep up with changing trends, tending to become overwhelmed by high false positives and failure to emerging fraud tactics. Machine learning algorithms differ in how well they can address such problems, and their accuracy depends largely on the type of data they are tested against.
This study aims to solve these issues by comparing the productivity of several machine learning procedures- Random Forest, Decision Tree, Naïve Bayes,

Logistic Regression and LSTM- in identifying credit card fraudulent transactions. It also checks how SMOTE (Synthetic Minority Oversampling Technique) can help avoid class skew resulting from creating more examples belonging to the minority class, hence enhancing the capability of the model to recognize infrequent cases of fraud. The objective is to determine which approaches, with or without SMOTE, provide the most precise and reliable performance, eventually helping to develop better and smarter fraud detection systems.

1.5 Research Objectives

This study is concerned with the improvement and assessment of machine learning techniques for recognizing fraud in credit card datasets that suffer from serious class imbalance. To achieve this purpose, the research identifies the focusing on clear objectives:

1. To train and test several machine learning techniques – like Random Forest, Decision Tree, Naïve Bayes, Logistic Regression, and Long Short-Term Memory (LSTM) to discover counterfeit transactions in credit card payments.
2. To investigate how highly imbalanced dataset, where genuine transactions vastly outweigh fraudulent ones, affects the reliability and accuracy of these algorithms.
3. To apply the Synthetic Minority Over-sampling Technique (SMOTE) in order toward alleviate the uneven class distribution problem by over-sampling the minority class to create more instances in the dataset, thus hoping to improve model performance in fraud detection
4. To assess and variation the outcomes of the proposed frameworks under two circumstances– pre and post SMOTE by comparing evaluation parameters like accuracy, precision, recall. And F1-score to realize the impact related to data balancing on that system results.

5. To identify the most suitable machine learning algorithm and class balancing method for possible use in real world credit card fraud information for detection purpose.

These aims are meant to direct the research towards developing an efficient, adaptive, and accurate fraud detection system that will address the needs of contemporary financial systems.

1.6 Scope of the study

This thesis is centered on applying supervised machine learning approaches to determine scam-related credit card activities. It utilizes a freely accessible dataset consisting of labelled transaction records, where each records, is classified as either genuine or fraudulent. This work encompasses the training and performance evaluation of five selected models: Random Forest, Decision Tree, Naïve Bayes, Logistic Regression, and Long Short-Term Memory (LSTM).

To deal with such problem of data imbalance when fraudulent transactions are far outnumbered by legitimate transactions- the SMOTE (Synthetic Minority Over-sampling Technique) technique is selectively implemented to the Random Forest and LSTM models. It is done in order to test how balancing data performs on more complicated or deep learning models. Others models are tested without SMOTE in order to see their baseline performance.

The purview of this thesis is restricted to the application of supervised learning methods alone. More sophisticated techniques like unsupervised learning, anomaly detection, or real time fraud detection systems are not explored in this research work. In addition, though the research yields useful information regarding model performance and data management, it is not an exercise in deploying the models into a real time production setting.

This study serves as a foundational study that can be extended in the future by integrating advanced methods, such as ensemble models, real-time detection, or integration with financial systems, to boost the practical utility of fraud identification systems.

1.7 Signification

This research holds significant value for financial institutions, banks, and payment service providers by contributing to more effective credit card fraud detection. Through comparing in a structured fashion multiple machine learning models and exploring the influence of data-equalization strategy such as SMOTE, the study looks for refine the accuracy as well as reliability of fraud identification. Improved identification methods not only help minimize financial losses caused by fraudulent transactions but also strengthen customer trust and confidence in electronic payment systems.

Moreover, the knowledge acquired from this research establish a base for developing smarter, evidence based fraud prevention tools that can adjust to evolving fraud sequence. The outcomes of this study have practical implications, offering guidance on selecting appropriate machine learning models and data pre-processing strategies that can be implemented in field based product detection frameworks. Ultimately, this work supports the ongoing efforts to safeguard financial networks and protect consumers in an increasingly digital economy.

1.8 Application and Misuse

Financial institutions, payment gateways, and online retailers employ credit card fraud detection tools to scrutinize every transaction as it happens. By combining standard algorithms like logistic regression, decision trees, and random forests with more sophisticated LSTM networks that use SMOTE to balance rare fraud cases, these solutions evaluate data points such as purchase amount, merchant type, location, and time. Should the system spot an out-of-the-ordinary transaction (for instance, a high-value charge from abroad), it can instantly block the payment, flag it for human investigation, or request extra verification, thereby curbing losses and protecting both cardholders and businesses. However, without clear rules and ethical oversight, these fraud-fighting systems can backfire. Relying too heavily on automated judgments often produces false alarms, denying legitimate purchases and frustrating customers especially those whose spending habits fall outside the norm. Furthermore, the same pattern-analysis methods could be exploited to track people’s buying behavior or make unfair lending decisions, unless strict controls govern who can access and act on the data.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

Credit card fraud has is increasingly a serious hurdle in the digital age given the growing dependence on digital and virtual financial transactions. Although e-commerce, mobile banking, and contactless payments have made it more convenient for the customers, they have simultaneously provided new channels for fraudulent activities. As the fraudulent approaches keep changing and becoming sophisticated, the conventional rule based detection tools are not able to effectively identify new patterns. As a result, there has been an increasing trend towards data driven methods particularly those informed by machine learning which are able to process historical transaction data and better identify abnormal or suspicious behavior.

In the last three years, numerous research studies have discovered the adoption of machine learning models to detect fraud by availing themselves of their ability to process massive datasets and detect faint patterns that may indicate fraudulent transactions. Approaches such as Random Forest, Decision Tree, Naive Bayes, Logistic Regression, and Deep Learning based models namely LSTM (Long Short-Term Memory) have been extensively studied and applied. Apart from model building, researchers have also overcome issues like class imbalance where actual transactions greatly exceed fraudulent ones by using techniques like SMOTE (Synthetic Minority Oversampling Technique) to improve model performance.

2.2 Different approaches for detecting fraud

Credit card fraud detection has seen a great advancement over the years, from rule driven and manual system to machine learning and hybrid methods. This methods can be classified into the following in general:

2.2.1 Traditional Methods

Traditional fraud detection relies on predefined rules and statistical profiling to identifying fraud in credit card:

1. Rule-Based Approach

The rule based method is one of the oldest and most classical techniques employed for credit card fraud detection. It execute according to the principle of applying pre-established rules examples limits on transaction amounts, numbers of transactions, or abnormal geographic activity to identify potentially suspicious behavior. These rules usually stem from historical data and professional institution.

Although simple and easy to apply rule based systems are static in nature. They do not adapt to changing fraud patterns, rendering them ineffective when pitted against emerging and advanced fraud schemes. Since fraudsters develop new schemes, the system tend to miss emerging patterns, resulting in case omissions and high false positive rates where genuine transactions are incorrectly flagged. On top of that, rule based detection is followed by time consuming manual reviews in many instances. Such manual reviews are non-scalable in high volume transactions. All these limitations have underpinned calls for more dynamic and smart systems. The sector has since turned towards machine learning model that evolves through data automatically as well as respond to new fraud behaviors.

2. Probabilistic and statistical approach

Statistical and probabilistic methods for credit card fraud detection construct models of typical transaction behavior utilizing methods like fitting univariate or multivariate distributions, computing statistical distance (e.g., Mahalanobis distance), or using Bayesian methods like Naive Bayes and Hidden Markov Models - to classify each new transaction with a likelihood or risk score. Transactions that belong to the tail of an experienced distribution or that have low transition probability in a sequence are identified as possible fraud. These techniques provide transparent, interpretable measures and they are based on firm mathematical grounds, but they rely on data distribution hypotheses and feature independence assumptions, tend to involve extensive feature engineering, and needs to be regularly updated to match changing user behaviors and techniques.

2.2.2 Machine Learning Approach

Machine learning has also been a very successful tool used to identify credit card fraud due to its flexibility to respond to changing trends. Supervised learning algorithms namely Random Forest, Naive Bayes, Decision Tree, and Logistic Regression are trained on labelled transaction data, thus being able to discriminate between real and fraudulent behavior based on regularities learned from historical data.

These models are great at identifying intricate patterns in big data and can generalized well to catch unseen cases of fraud. A significant problem here, though, is the skewed class distribution issue where the deceptive transactions are a minor fraction of the data. To counter this, strategies such as SMOTE (Synthetic Minority Over-sampling Technique) are usually used to optimize model performance by balancing the dataset.

2.2.3. Deep Learning Approach

Deep learning, being a form of machine learning, uses complex neural network structures to capture complex data relationships. Long Short-Term Memory (LSTM) networks have proven to be especially useful in fraud detection within sequential transaction data because they can learn temporal dependencies.

Deep learning algorithms are able to pick up on implicit, non-linear relationships and update themselves in response to changing fraud behaviors without human feature engineering. They have high accuracy but introduce challenges related to higher computational needs, longer training times, and less interpretability than traditional models.

These three models methods are the basic of current credit card fraud detection systems. The progression from static rules to intelligent learning models is a result of increasing sophistication in fraud schemes and the necessity for stronger, scalable, and adaptive detection algorithms.

2.3 Related Work

Detecting credit card fraud has become very important because online transactions are growing fast, and fraudsters are getting smarter. Table 1 demonstrate the comparison of some previous work based on different machine learning models with their accuracy.

B Dharma et al. [1] presented a study proposing an ML-based system for detecting credit card frauds. The dataset of European cardholders was used in their investigation, and Using principal component analysis (PCA) or feature selection, 28 features were derived from original attributes. In the created model, the dataset is separated into train and test data in 70:30 for training and testing purposes. This research primarily examined the accuracy of various machine learning models, with KNN achieving 86%, NB achieving 82%, and the hybrid ML model (SVM+LR) achieving 97%.

Sugandha Jain et al. [2] suggested this study, which offers a model for identifying credit card fraud. To increase the accuracy and efficiency of the proposed framework, a systematic algorithm has been implemented into place. The dataset was examined using the exploratory data analysis (EDA) method. Graphs were plotted using key features to show how they relate to one another and how they help identify credit card fraud. Following EDA, division of dataset was done in 70: 30 for training and testing. The maximum accuracy (95%) and precision (100%) were attained by the proposed model.

Using a Competitive Swarm Optimization (CSO) algorithm for feature selection, A. Gajakosh et al. [3] introduced a fraud detection method for credit card transactions. To refine the accuracy of fraud detection, their work presented a CSO-SVM hybrid model that makes use of unsupervised learning. The European credit cardholder dataset, which comprises 284,807 transactions from September 2013, was used to assess the model. Only 492 transactions (0.17%) were fraudulent, whereas 99.83% were real, demonstrating the dataset's significant class imbalance. The analysis showed that using CSO algorithm for selection of relevant features considerably enhanced performance, resulting in an amazing 99.88% accuracy using the Support Vector Machine (SVM) model.

Chaitanya et al. [4] proposed a credit card fraud detection system based on Hidden Naïve Bayes and Bayesian Belief Network. Both models were examined using the "Abstract dataset for credit card fraud detection," which consists of 11 characteristics and 3075 occurrences. The study focused mostly on accuracy, with HNB scoring 86.87% and BBN scoring 89.59%.

Vishnu R. Sonwane et al. [5] conducted a detailed study of machine learning methods for credit card fraud detection using the Kaggle Credit Card Fraud Detection Dataset [5]. This research aims to identify acceptable machine learning approach for fraud detection in credit card using decision trees, random forests, and neural networks, with neural networks providing the greatest accuracy (99.96%).

Another study by Mohit Beri et al. [6] analyses the detection of credit card fraud using two well-known machine learning techniques: artificial neural networks (ANNs) and XGBoost. In addition, several ML models namely

Random Forest, CatBoost, and LightGBM are used. Cross-validation approaches, such as k-fold cross-validation [6], will ensure the dependability and generalizability of the models in this study. This involves dividing the data into various folds, training the model on multiple subsets, and assessing its performance on the final fold. All accessible models in this study, ANN and XGBoost, achieve the maximum accuracy (96.9% and 92.7%, respectively).

Negar Nasiri et al. [7] examine credit card fraud detection using supervised machine learning algorithms. The LR, RF, and DT models are assessed according to various measures based on accuracy, precision, recall, and F-measure. This research uses Prof. Hoffmann's German credit card fraud dataset, which has 1000 features and 20 categorical variables. Seven of these 20 features are numerical, while thirteen are qualitative. Random Forest exceeds the other two models in both precision and accuracy.

Aditi Singh et al. [8] worked on detecting credit card fraud using machine learning. They used a dataset which is highly imbalanced taken from Kaggle shared by Brandon Harris. The dataset contained specifications such as amount of money spent in transaction, average spending in last 24 hours, and transaction time. The ratio of training and testing taken was 80:20.Among the models which was implemented CatBoost gave the highest accuracy of 99.87%.

Reference	Year	Dataset	Model Used	Accuracy
[1]	2025	European Cardholders Dataset	KNN NB SVM+LR	86% 82% 97%
[2]	2024	Synthetic Financial Datasets (FraudTrain.csv FraudTest.csv)	Proposed Model	95%
[3]	2024	European Cardholders Dataset	CSO-SVM	99.88%
[4]	2024	Abstract dataset	HNB Model BBN Model	86.87% 89.59%
[5]	2024	European Cardholders Dataset	DT RF NN	99.92% 99.95% 99.96%
[6]	2024	-----------	ANN XGBoost RF CatBoost LightGBM	96.9% 92.7% 90.8% 91.2% 91.8%
[7]	2023	Germen Credit Card Fraud Dataset	LR RF DT	72% 76% 72%
[8]	2022	Synthetic Financial Datasets (FraudTrain.csv FraudTest.csv)	LR DT RF Catboost	93.70% 99.40% 99.60% 99.87%

Table 2.1 Comparison table of previous work with their accuracy

2.4 Handling Class Imbalance

Handling asymmetric class distribution is an important process in machine learning, especially if one class is far more common than the other. Class imbalance can lead to biased models and poor performance when it comes to detecting the minority class. Various mechanisms are available to solve this challenge and make the model fair and accurate.

2.4.1 Under-sampling the Majority Class

Under-sampling involves lessening the frequency in the majority class to balance the dataset. It is an effective when the majority class contains numerous redundant or similar cases. But, it has the drawback of losing potentially important information, which could adversely affect the model's generalization on unseen data.

2.4.2 Oversampling the Minority Class

Oversampling boosts the number of instances in the minority class to equalize the majority class. It is commonly achieved by repetitive duplication of minority class examples at random. Though it assists in balancing the data, it can cause overfitting, since the model would learn to memorize duplicate samples rather than generalize.

2.4.3 SMOTE (Synthetic Minority Over-sampling Technique)

SMOTE is a sophisticated oversampling method that synthesizes data for the under-represented class examples instead of just replicating them. It proceeds to interpolate between the present minority class instances and their nearest neighbours in the feature space. An example is the detection of credit card fraud, where legitimate transactions overwhelm fraudulent ones, SMOTE assists by creating artificial fraud samples from existing cases of fraud. This enriches variety but realistic examples of the dataset, supporting the model's learning process stronger decision margins. By refining the model's recognition capabilities infrequent fraudulent regularities, SMOTE avoids false negatives and enhances overall performance. Nevertheless, it must be used cautiously to prevent overfitting as well as to maintain the original data distribution.

2.4.4 Class Weighting

Class weighting modifies the loss function at training to assign greater weight to the minority class. This method works well with weighted loss function-supported algorithms, including logistic regression, support vector machines, and neural networks. It makes the model more focused on the minority class at training time, enhancing its capacity to label those instances appropriately.

2.4.5 Use of Ensemble Methods

Ensemble methods include Balanced Random Forest, Easy-Ensemble, or AdaBoost trained different models on various balanced subsets of data and combine them. These increase the effectiveness of the model by exploiting the benefits of numerous learners and minimizing the bias likely to be caused by class imbalance.

2.4.6 Anomaly Detection Perspective

In cases of extreme imbalance, the minority class may be handled as an outlier or anomaly. Employing algorithms for anomaly detection enables the model to learn the normal behaviour (over-represented class) and mark deviations (under-represented class) as noteworthy, something highly effective in areas such as fraud detection or rare disease diagnosis.

2.4.7 Use of Proper Evaluation Metrics

When working with imbalanced datasets, just using accuracy can be deceptive. Parameters like precision, recall, F1-score, and AUC-ROC gives a better elucidate the performance of the model, particularly in accurately predicting the minority class without over-estimation due to the majority class.

2.4.8 Data Augmentation (for images/text)

Data augmentation entails generating altered form of the minority class data to boost its volume and variance. In image data, for instance, this could entail rotations, flips, or colour changes. In text, it may entail synonym replacement or back-translation. The method has been found to work especially well in domain including image recognition and natural language processing.

2.5 Summary

Credit card fraud detection has progressed from static, logic driven systems relying on expert-defined thresholds for transaction amounts or locations to more sophisticated statistical and probabilistic models that assign risk scores based on learned data distributions and sequential behavior patterns. The limitations of these traditional methods, including high false-positive rates and inflexibility, spurred the adoption of supervised machine learning approaches (including Decision Trees, Random Forests, Naïve Bayes, and Logistic Regression), which learn complex, non-linear relationships from labeled transaction data but must contend with severe class imbalance. More recently, deep learning approaches, particularly LSTM networks, have demonstrated superior ability to capture temporal dependencies in transaction streams, albeit with increased demands for data, computation, and interpretability. Across both machine learning and deep learning paradigms, procedures like SMOTE have become essential for synthetically balancing the minority (fraud) class, reducing false negatives and enhancing overall detection performance.

CHAPTER 3

METHODOLOGY

In this thesis, Methodology displays the overall workflow of paper with respect to credit card fraud detection system which examines user expenditure behavior to discover the unauthorized transactions. It compares several machine learning algorithms—Logistic Regression, Decision Trees, Random Forest, Naïve Bayes, and LSTM—to determine the most effective model for credit card merchants in detecting fraud [9]. Fig. 3.1 depicts the overall workflow of the proposed approach.

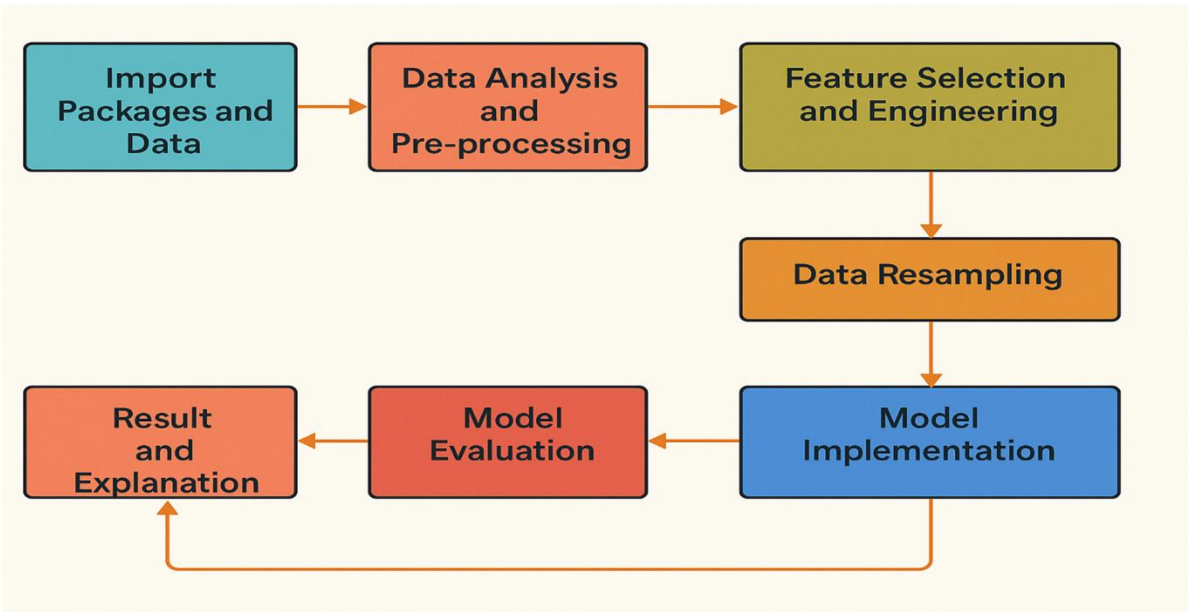


Fig.3.1 Workflow Diagram

3.1 Dataset Description

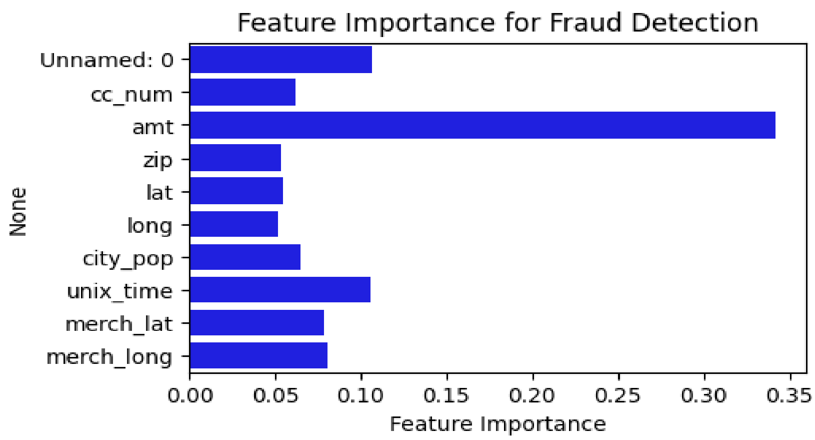
We are using Sparkov Brandon Harris dataset from Kaggle for detection of fraud, which is imbalanced in nature, having only 0.5% transactions marked as fraudulent. These datasets consist of two files: FraudTrain.csv and FraudTest.csv spanning from January 1, 2019 to December 31, 2020 with both original and fraud transactions. This dataset has 23 unique features and 1604294 total records with target variable 'is_fraud'.

3.2 Data Preprocessing

Data from real world sources often include noise, inappropriate values, or poorly formatted values, requiring data preprocessing to improve model accuracy and efficiency. We handled missing values and used One-Hot Encoding to change categorical variables including transaction type and time-stamp into numerical values, which improved prediction accuracy.

3.3 Feature Selection

Feature selection involves selecting important features, removing irrelevant features by dropping unnecessary columns, applying standardization, normalization and handling outliers to enhance model performance. In this work we select some appropriate features which contribute meaningfully in our work, like transaction amount, merchant category, latitude, longitude etc. to co-relate the fraudulent transaction and genuine transaction which shows in fig. 3.2.



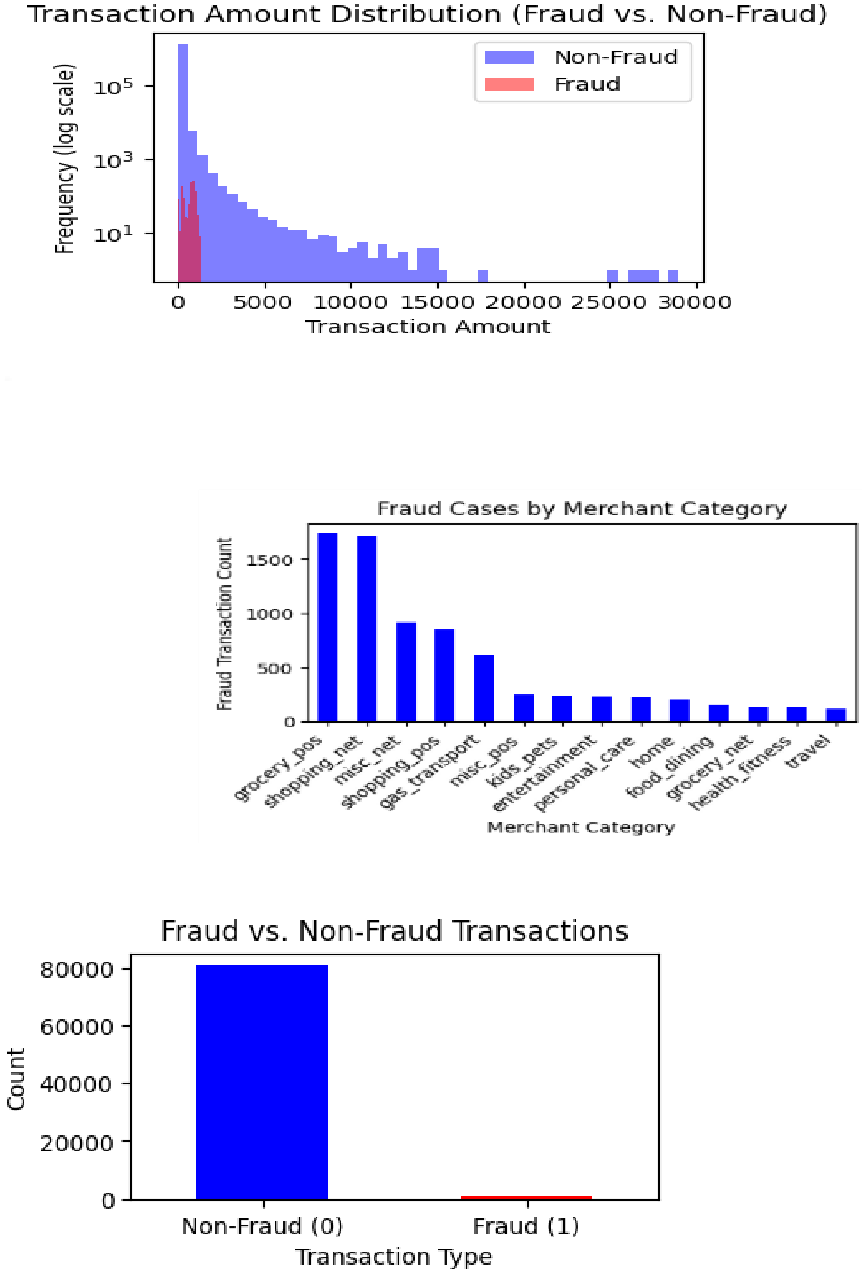


Fig. 3.2 Selecting Important Features for fraud detection

3.4 Data Resampling

When fraudulent transactions are rare, the dataset becomes imbalanced, so we need to balance it using data resampling. Two common methods for this are undersampling and oversampling. To balance a dataset, undersampling reduces the over-represented class and oversampling raises the under-represented class using techniques like random oversampling and SMOTE. The extremely uneven dataset results in biased models that perform poorly in minority classes. SMOTE engages with this by constructing artificial examples of the minority class. After applying SMOTE, LSTM model gives the better performance as compared to the accuracy of same model with imbalanced dataset.

3.5 Model Implementation

Implementation of model refers to the process of putting a plan or idea into effect to a model whose representation of a real world process. This study analyses 5 different models.

1. Random Forest – A Random Forest is a tree-based approach that includes creating many trees and merging them with the output to improve the model's generalization ability [10]. Fraud detection in credit card, Random Forest is used as an ensemble approach that handles big datasets and aggregate multiple decision trees to boost predictive performance and suppress overfitting.

2. Decision Tree – A Decision is a supervised learning method [11] that is commonly used for categorization tasks. It follows a recursive approach, where data is repeatedly divided based on specific features until it reaches a final classification.

3. Logistic Regression – Logistic Regression is a basic but effective supervised learning method that is often used for binary classification tasks, such as detecting fraudulent and non-fraudulent credit card transactions [11, 12]. The model utilizes past data to assess the likelihood of a fraudulent transaction.

4. Naïve Bayes Classifier – It is a simple and smart approach that uses probabilistic model based on Bayesian theory, which determines the most likely classification by calculating probabilities. This approach estimates unknown probabilities using observed data and incorporates prior knowledge to refine predictions.

5. LSTM – It is a type of Recurrent Neural Network (RNN) designed to accept sequential input and solve the diminishing gradient problem common to ordinary RNNs. LSTM networks for detecting credit card fraud can be particularly effective because of their capacity to record temporal association in transaction data (fig. 3.3).

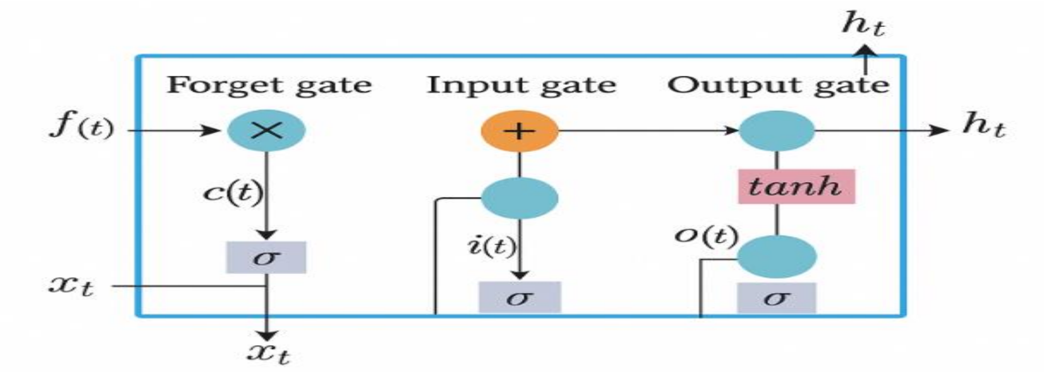


Fig.3.3 Architecture of LSTM

LSTM cells have two internal vectors- a memory cell and a hidden state, which are updated every time step by three learned gates:

1. Forget gate - determines what elements of the last memory to retain.
2. Input gate - determines what new materials to write to the memory.
3. Output gate – figures out the portion of the updated memory to use for the next hidden state

A fraud detection model will usually stack a single or double such LSTM layers (each of 64-128 units and optional bi-directionality), add dropout between, and conclude with a single sigmoid neuron that produces the fraud probability. Training is optimized for binary cross entropy with the Adam optimizer and uses early stopping on validation AUC to avoid overfitting.

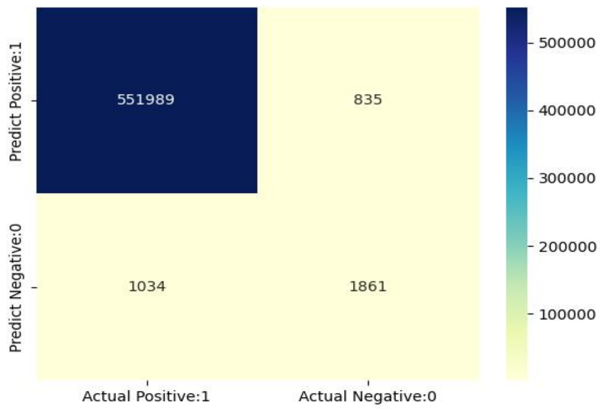
CHAPTER 4

RESULTS AND DISCUSSION

The model is analyzed using diverse evaluation parameters for detecting credit card fraud to check how model better classified transaction is fraudulent or genuine:

4.1 Evaluation Metrics - The models are assessed using a confusion metrics and a set of standard performance metrics computed on a 70:30 train test split:

4.1.1 Confusion Matrix - A confusion matrix will offer us a clear depiction of classification model structures performance and the varieties of errors it produces. It provides an overview of correct and wrong estimates, broken down by category. Figures 4.1 and 4.2 illustrate a confusion matrix for Random Forest and LSTM with an imbalanced dataset and after balancing the dataset using SMOTE.



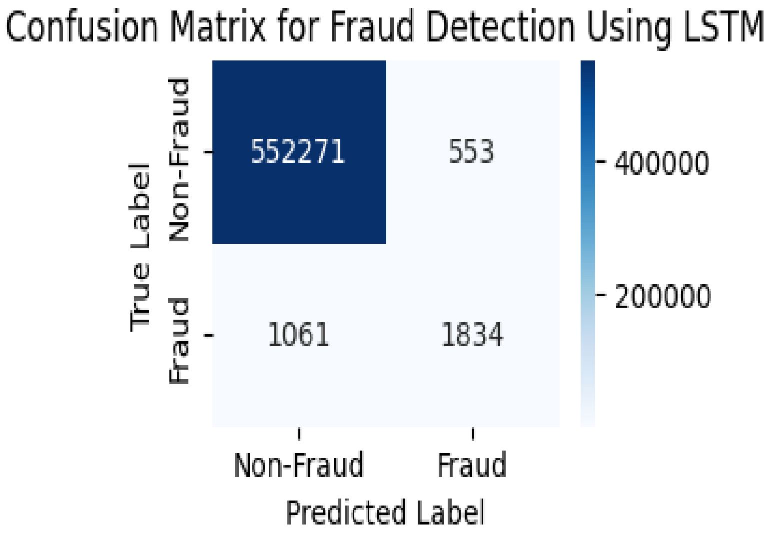


Fig.4.1 Confusion matrix of Random Forest and LSTM with imbalanced dataset

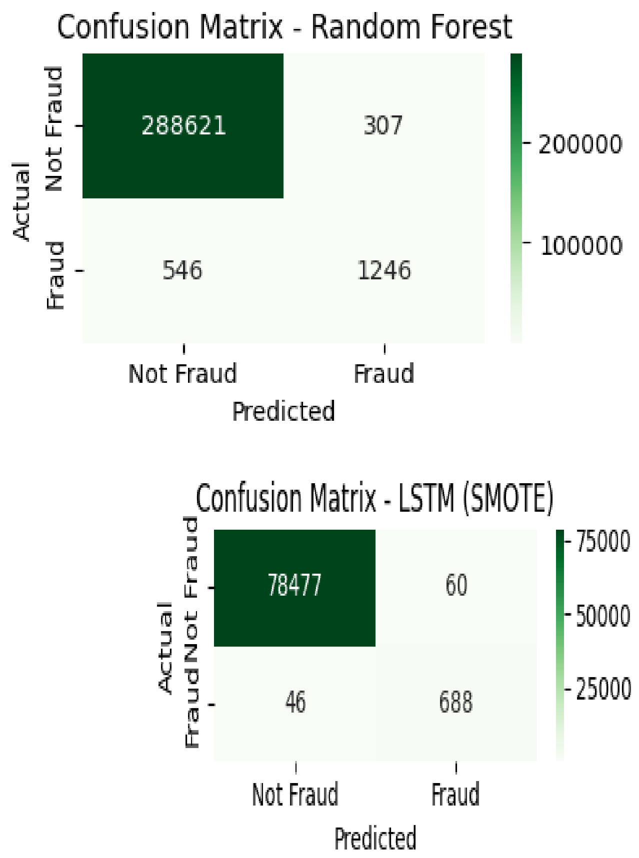


Fig.4.2 Confusion matrix of Random Forest and LSTM using SMOTE

4.1.2 Performance Metrics - Based on the earlier mentioned dataset, we check the performance of different ML and DL algorithms on a 70:30 training and testing dataset. For the comparison of models, accuracy, positive predicted value, recall or sensitivity, and F1-score are used as performance indicators. Additionally, the computational efficiency of each model is evaluated in order to compare resource utilization. The performance metrics can be described as following:

Accuracy: Accuracy is defined as the fraction of correct predictions [11].

$$\textbf{Accuracy} = \frac{\mathrm{TP+TN}}{\mathrm{TP+TN+FP+FN}}$$

Positive Predictive Value (or) Precision: Precision refers to the fraction of affirmative cases that are accurately detected [11].

$$\textbf{Precision} = \frac{\mathrm{TP}}{\mathrm{TP+FP}}$$

Recall/Sensitivity: It is the percentage of true positive instances correctly detected [11].

$$\textbf{Recall} = \frac{\mathrm{TP}}{\mathrm{TP+FN}}$$

F1 Score: The F1 Score is defined as the harmonic mean of precision and recall values in a classification task [11].It is the percentage of true positive instances correctly detected [11].

$$\boldsymbol{F}\mathbf{1}\ \textbf{Score} = \frac{2 * Recall * Precision}{Recall + Precision}$$

Where,

TP= Valid Positive Outcomes

TN = Valid Negative Outcomes

FP= Type 1 Error

FN = Type 2 Error

ROC: Plotting the True Positive Rate (TPR) in contrast with the False Positive Rate (FPR) creates a curve that illustrates a classification evaluation of model behaviour across all decision boundaries.

AUC (Area under the Curve): A single scalar measurement reporting the area under the ROC curve. It measures the framework's capacity to set apart classes, with values ranging from 0 - 1.

4.2 Comparative Analysis of Models With and Without SMOTE

Table 4.1 provides a side-by-side comparison of different models evaluated through performance indicators such as Accuracy, Precision, Sensitivity, F1-Score, and ROC/AUC, using an imbalanced dataset where random forest shows the best performance matrix with 99.77% accuracy. When the dataset is balanced using the SMOTE technique, the LSTM model shows significant improvement across all performance metrics with accuracy 99.87%, as presented in Table 4.2, compared to its performance on the imbalanced dataset.

Performance Without SMOTE

Models perform well on accuracy but poorly on recall, indicating failure to identify many fraudulent transactions. Random Forest and LSTM perform best among all models but still show bias toward the majority class.

Model	Accuracy	Precision	Recall	F1-Score	ROC-AUC
RF	99.77%	99.80%	99.68%	73.58%	98.60%
DT	99.66%	69.03%	64.28%	66.57%	82.07%
NB	99.12%	28.76%	46.87%	35.64%	85.78%
LR	94.55%	06.98%	76.72%	12.80%	86.28%
LSTM	99.71%	76.83%	63.35%	69.00%	97.00%

Table 4.1 Performance on Imbalanced Dataset

Performance With SMOTE

SMOTE significantly improves recall and F1-scores across all models. LSTM shows the highest performance, demonstrating its capability to detect complex patterns.

Model	Accuracy	Precision	Recall	F1-Score	ROC-AUC
RF	99.71%	77.45%	70.85%	74.00%	98.24%
DT	96.24%	6.91%	70.16%	12.58%	83.37%
NB	99.42%	29.46%	36.69%	32.68%	82.41%
LG	89.23%	0.22%	5.92%	0.42%	47.73%
LSTM	99.87%	91.98%	93.73%	92.85%	99.75%

Table 4.2 Performance After SMOTE

4.3 Result Evaluation

When we first ran the models on the skewed dataset, Random Forest and LSTM both showed almost perfect accuracy (99.77 % and 99.71 %) and strong ROC-AUC values (98.60 % and 97.00 %), but they missed a significant share of actual frauds—LSTM detected only 63.35 % of fraud cases despite RF's 99.68 % recall—and simpler methods like Decision Trees, Naive Bayes, and Logistic Regression struggled with either precision or recall due to the overwhelming number of genuine transactions. Introducing SMOTE to even out the classes boosted every model's ability to spot fraud, with LSTM benefiting the most: its recall soared to 93.73 %, its F1-score climbed to 92.85 %, and its accuracy and ROC-AUC both rose to nearly 99.9 %. Random Forest also saw gains in recall and F1 but couldn't quite keep pace with the balanced performance of LSTM, while the basic algorithms still lagged behind. This shows that class balancing is crucial for catching fraud and that, once corrected for imbalance, LSTM offers the strongest detection capability.

CHAPTER-5
CONCLUSION

5.1 Conclusion

This study illustrates how different machine learning methods, including Random Forest, Decision Tree, Naive Bayes, Logistic Regression, and Long Short Term Memory (LSTM), can be utilized in order to identify fraud. These methods possesses high capability to enhance how effectively we can ascertain fraud cases. Outcomes of various ML methods in the form of graph is represented in fig. 6.

This study demonstrates that machine learning can effectively detect fraudulent transactions, with Random Forest and LSTM showing promising results in both imbalance dataset and balanced dataset using SMOTE.

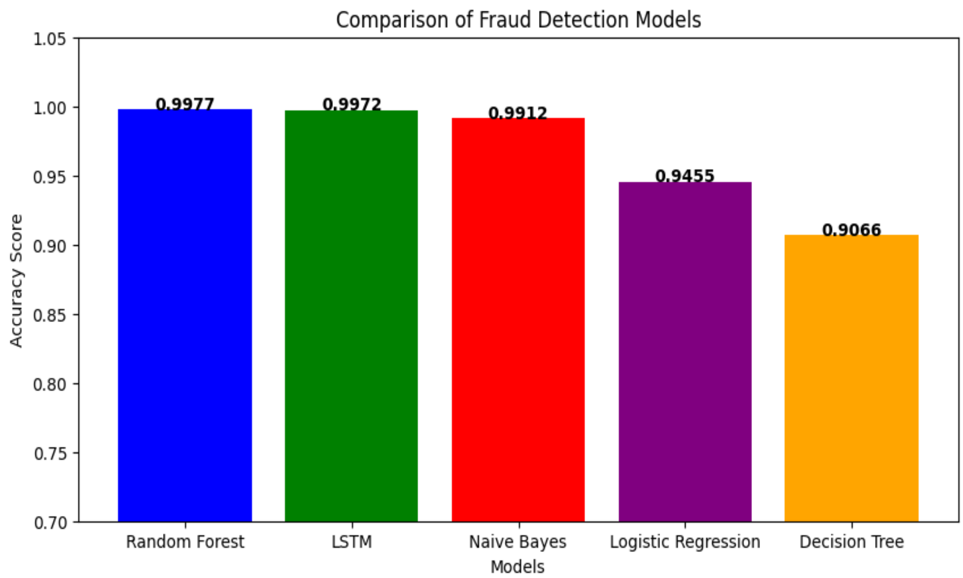


Fig. 5.1 Performance analysis of different ML Algorithm

5.2 Limitations

- Models are tested on a static dataset; real-time validation is required.
- The anonymized dataset limits exploration of feature engineering.
- LSTM requires high computational resources.

5.3 Future Work

- Integrate additional data sources such as user location or device fingerprints.
- Explore hybrid and ensemble deep learning approaches.
- Develop real-time fraud detection systems with adaptive learning.
- Test on industry-grade, non-anonymized datasets.

REFERENCE

[1]. Bhukya Dharma, Dr D Latha, “Fraud Detection in Credit Card Transactional Data using Hybrid Machine Learning Algorithm,” Proceedings of the 6th International Conference on Mobile Computing and Sustainable Informatics (ICMCSI-2025) IEEE Xplore Part Number: CFP25US4-ART; ISBN: 979-8-3315-2266-7, 2025, pp. 1-6, doi: 10.1109/ICMCSI64620.2025.10883549.

[2]. Sugandha Jain, Nivedita Sharma, and Manni Kumar, "FraudFort: Harnessing Machine Learning for Credit Card Fraud Detection," *2024 First International Conference on Technological Innovations and Advance Computing (TIACOMP)*, Chandigarh, India, Mar. 2024, pp. 1-6, doi: 10.1109/TIACOMP64125.2024.00017.

[3]. A Gajakosh, R A Reddy, M M adnan, G Rajalaxmi, Pramodhini R, "Fraud Detection in Credit Card Using Competitive Swarm Optimization with Support Vector Machine," *2024 International Conference on Distributed Computing and Optimization Techniques (ICDCOT)*, 2024, pp. 1-4, doi: 10.1109/ICDCOT61034.2024.10515953.

[4]. G S Chaitanya, K Deepika, G S Prabhav, R B. Patil, and M. A. Jabbar, "Credit Card Fraud Detection using Hidden Naive Bayes and Bayesian Belief Network," *2024 IEEE 9th International Conference for Convergence in Technology (I2CT)*, Pune, India, Apr. 2024, pp. 1-6, doi: 10.1109/I2CT61223.2024.10544328.

[5]. Vishnu R. Sonwane, S Zanje, S Yenpure, Y Gunjal, Y Kulkarni, R Yeole,” Advanced Machine Learning Techniques for Credit Card Fraud Detection: A

Comprehensive Study,” 5th International Conference on Smart Electronics and Communication (ICOSEC 2024) IEEE Xplore Part Number: CFP24V90-ART; ISBN: 979-8-3315-0440-3, 2024, pp. 1-4, doi: 10.1109/ICOSEC61587.2024.10722667.

[6]. Mohit Beri, Kanwarpartap Singh Gill, Neha Sharma,” Enhancing Credit Card Fraud Detection: A Comparative Analysis of Machine Learning Models,” Proceedings of the International Conference on Sustainable Expert Systems (ICSES-2024) IEEE Xplore Part Number: CFP24VS6-ART; ISBN: 979-8-3315-4036-4, 2024, pp. 1-6, doi: 10.1109/ICSES63445.2024.10763059.

[7]. Q S Mirhashemi, Negar Nasiri, Mohd. R Keyvanpour, "Evaluation of Supervised Machine Learning Algorithms for Credit Card Fraud Detection: A Comparison," *2023 9th International Conference on Web Research (ICWR)*, 2023, pp. 1-6, doi: 10.1109/ICWR57742.2023.10139098.

[8]. Aditi Singh, Anoushka Singh, Anshul Aggarwal, Anamika Chauhan, “Design and Implementation of Different Machine Learning Algorithms for Credit Card Fraud Detection,” Proc. of the International Conference on Electrical, Computer Communications and Mechatronics Engineering (ICECCME) 16-18 November 2022, Maldives, pp. 1-6, doi: 10.1109/ICECCME55909.2022.9988588.

[9]. Lakshmi S. V. S. S., and S. D. Kavilla,”Machine learning for credit card fraud detection system,” International Journal of Applied Engineering Research 13, no. 24, 2018, pp. 16819-16824.s

[10]. Xuan, S., Liu, G., Li, Z., Zheng, L., Wang, S. and Jiang, C., 2018, March. Random forest for credit card fraud detection. In 2018 IEEE 15th International Conference on Networking, Sensing and Control (ICNSC) (pp. 1-6). IEEE

[11]. Indrani Vejalla, Sai Preethi Battula, Kartheek Kalluri, Hemantha Kumar Kalluri, “Credit Card Fraud Detection Using Machine Learning Techniques,” 2023 2nd International Conference on Paradigm Shifts in Communications Embedded Systems, Machine Learning and Signal Processing (PCEMS), 2023, pp. 1-4, doi: 10.1109/PCEMS58491.2023.10136040.

[12]. V. K. K. S., V. G. V. K., A. V. S., and P. K., “Credit Card Fraud Detection using Machine Learning Algorithms,” International Journal of Engineering Research & Technology (IJERT), vol. 9, no. 07, pp. 1526–1530, Jul. 2020.

DELHI TECHNOLOGICAL UNIVERSITY

(Formerly Delhi College of Engineering)

Shahbad Daulatpur, Main Bawana Road, Delhi-42

PLAGIARISM VERIFICATION

Title of the Thesis____

____

Total Pages ________________ Name of the Scholar____________________________________

Supervisor (s)

(1)____________________________________

(2)____________________________________

(3)____________________________________

Department____

This is to report that the above thesis was scanned for similarity detection. Process and outcome is given below:

Software used: _______________________ Similarity Index: ______, Total Word Count: ________

Date: ___________

Candidate's Signature **Signature of Supervisor(s)**

4thSEMTHESIS.docx

Delhi Technological University

Document Details

Submission ID

trn:oid:::27535:98227814

Submission Date

May 29, 2025, 1:05 AM GMT+5:30

Download Date

May 29, 2025, 1:06 AM GMT+5:30

File Name

4thSEMTHESIS.docx

File Size

1.7 MB

28 Pages

6,380 Words

37,983 Characters

7% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

Filtered from the Report

- Bibliography
- Quoted Text
- Cited Text
- Small Matches (less than 8 words)

Match Groups

44 Not Cited or Quoted 7%
Matches with neither in-text citation nor quotation marks

0 Missing Quotations 0%
Matches that are still very similar to source material

0 Missing Citation 0%
Matches that have quotation marks, but no in-text citation

0 Cited and Quoted 0%
Matches with in-text citation present, but no quotation marks

Top Sources

5% Internet sources
4% Publications
6% Submitted works (Student Papers)

Integrity Flags

0 Integrity Flags for Review

No suspicious text manipulations found.

Our system's algorithms look deeply at a document for any inconsistencies that would set it apart from a normal submission. If we notice something strange, we flag it for you to review.

A Flag is not necessarily an indicator of a problem. However, we'd recommend you focus your attention there for further review.

Match Groups

44 Not Cited or Quoted 7%
Matches with neither in-text citation nor quotation marks

0 Missing Quotations 0%
Matches that are still very similar to source material

0 Missing Citation 0%
Matches that have quotation marks, but no in-text citation

0 Cited and Quoted 0%
Matches with in-text citation present, but no quotation marks

Top Sources

5% Internet sources
4% Publications
6% Submitted works (Student Papers)

Top Sources

The sources with the highest number of matches within the submission. Overlapping sources will not be displayed.

1	Internet	
	www.mdpi.com	<1%
2	Publication	
	"Advances in Machine Learning and Big Data Analytics I", Springer Science and B...	<1%
3	Internet	
	www.coursehero.com	<1%
4	Submitted works	
	University of Cape Town on 2020-04-26	<1%
5	Internet	
	link.springer.com	<1%
6	Submitted works	
	Middlesex University on 2025-04-13	<1%
7	Internet	
	dokumen.pub	<1%
8	Internet	
	pmc.ncbi.nlm.nih.gov	<1%
9	Submitted works	
	Liverpool John Moores University on 2025-02-26	<1%
10	Internet	
	mdpi-res.com	<1%

11 Submitted works

Central Queensland University on 2024-09-04 <1%

12 Internet

ir.juit.ac.in:8080 <1%

13 Internet

studentsrepo.um.edu.my <1%

14 Submitted works

Liverpool John Moores University on 2025-05-15 <1%

15 Internet

www.researchgate.net <1%

16 Submitted works

Glasgow Caledonian University on 2025-01-03 <1%

17 Internet

arizona.openrepository.com <1%

18 Internet

ijpeds.iaescore.com <1%

19 Internet

5dok.net <1%

20 Publication

Aditi Singh, Anoushka Singh, Anshul Aggarwal, Anamika Chauhan. "Design and I... <1%

21 Publication

Araf Islam, Mohammad Abu Saleh, Afia Fairooz Tasnim, Md. Samiun, Syeda Kama... <1%

22 Publication

Dinesh Goyal, Bhanu Pratap, Sandeep Gupta, Saurabh Raj, Rekha Rani Agrawal, I... <1%

23 Submitted works

Middlesex University on 2021-01-08 <1%

24 Submitted works

University of Derby on 2020-09-11 <1%

25 Submitted works

University of Kent at Canterbury on 2023-08-16 <1%

26 Submitted works

University of Sunderland on 2024-12-12 <1%

27 Submitted works

University of Wales, Lampeter on 2023-09-14 <1%

28 Submitted works

Chandigarh University on 2024-09-01 <1%

29 Submitted works

Mepco Schlenk Engineering college on 2025-04-29 <1%

30 Publication

Mimusa Azim Mim, Nazia Majadi, Peal Mazumder. "A soft voting ensemble learni... <1%

31 Submitted works

Monash University on 2023-10-19 <1%

32 Submitted works

The University of the West of Scotland on 2023-12-15 <1%

33 Submitted works

University of Hertfordshire on 2023-08-27 <1%