Credit Card Fraud Detection
Using Machine Learning

Project Report Submitted in Partial Fulfilment of the Requirements for the Degree of

Bachelor of Technology (Hons.)

in

Computer Science and Engineering

Submitted by

ANKESH: (Roll No. 2021UGCS058)

BETHA SUSHMA: (Roll No. 2021UGCS120)

Under the Supervision of
Dr. R. R. Suman
Associate Professor

Department of Computer Science and Engineering
National Institute of Technology Jamshedpur

April, 2024

CERTIFICATE

This is to certify that the report entitled “**Credit Card Fraud Detection Using Machine Learning**” is a bonafide record of the **Project** done by **ANKESH** (*Roll No*.: **2021UGCS058**) and **BETHA SUSHMA** (*Roll No*.: **2021UGCS120**) under our supervision, in partial fulfilment of the requirements for the award of the degree of **Bachelor of Technology (Hons.)** in **Computer Science and Engineering** from **National Institute of Technology Jamshedpur.**

Dr. R. R. Suman (Guide)

Associate Professor

Computer Science and Engineering

***Date*:** 04 April 2024

DECLARATION

We certify that the work contained in this report is original and has been done by us under the guidance of our supervisor. The work has not been submitted to any other Institute for any degree. We have followed the guidelines provided by the Institute in preparing the report. We have conformed to the norms and guidelines given in the Ethical Code of Conduct of the Institute. Whenever we have used materials (data, theoretical analysis, figures, and text) from other sources, we have given due credit to them by citing them in the text of the report and giving their details in the references. Further, we have taken permission from the copyright owners of the sources, whenever necessary.

Signature of the Students

2021UGCS058	**ANKESH**	**Sign**
2021UGCS120	**BETHA SUSHMA**	**Sign**

ACKNOWLEDGEMENT

We would like to express our deepest gratitude to our faculty supervisor, Dr. R. R. Suman, for his invaluable guidance, unwavering support, and insightful feedback throughout the course of this project.

We would also like to extend our appreciation to this institute for providing access to resources and data necessary for conducting this study. Additionally, we would like to thank our peers and colleagues for their constructive discussions and encouragement.

This project would not have been possible without the collective effort, and we are deeply thankful for the contributions of all those who played a role, no matter how big or small.

ANKESH	2021UGCS058
BETHA SUSHMA	2021UGCS120

ABSTRACT

The "Credit Card Fraud Detection using Machine Learning" project endeavours to combat fraudulent activities within financial transactions by leveraging the capabilities of machine learning. In the landscape of financial security, where the detection and prevention of fraudulent transactions are paramount, the development of accurate predictive models holds substantial importance. This project utilizes Python libraries such as NumPy, Pandas, Matplotlib, and Scikit-learn to construct and assess robust fraud detection models.

The project initiates by gathering historical credit card transaction data, serving as the basis for training and validating machine learning models. NumPy and Pandas facilitate data manipulation and preprocessing tasks. Leveraging the Scikit-learn library, a range of machine learning algorithms are deployed and assessed for their efficacy in identifying fraudulent transactions. Matplotlib is employed for data visualization, facilitating the creation of informative visualizations to comprehend transaction patterns, model predictions, and performance metrics.

In summary, the "Credit Card Fraud Detection using Machine Learning" project underscores the potency of machine learning methodologies and Python libraries in addressing intricate real-world challenges. It illustrates the potential for accurate fraud detection, providing invaluable insights for financial institutions, merchants, and security analysts in safeguarding against fraudulent activities.

LIST OF CONTENTS

LIST OF ABBREVIATIONS

KNN	K Nearest Neighbours
IG	Information Gain
E	Entropy
GI	Gini Index
LSTM	Long Short-Term Memory

CHAPTER 1
INTRODUCTION

1.1 INTRODUCTION

In the realm of financial transactions, the prevalence of fraudulent activities poses a significant challenge to the integrity of credit card systems and the trust of consumers and businesses alike. As technology evolves, so do the methods employed by fraudsters, necessitating advanced techniques for detection and prevention. Amidst this landscape, the fusion of machine learning and financial security emerges as a promising solution.

The project titled "Credit Card Fraud Detection using Machine Learning" embarks on a journey to fortify the defences against fraudulent transactions by harnessing the power of data science and computational models. It explores the intricate interplay between data patterns, transaction dynamics, and predictive algorithms to discern fraudulent activities within credit card transactions.

Project Overview

The primary aim of this project is to develop robust machine learning models capable of detecting fraudulent credit card transactions. By analysing historical transactional data, elucidating the underlying patterns indicative of fraud, and employing state-of-the-art algorithms, we endeavour to address the pressing question: "How can machine learning aid in identifying and mitigating credit card fraud?"

Motivation

The motivation driving this project is multifaceted. The integrity of financial transactions is paramount for maintaining trust in the banking and commerce sectors. Effective fraud detection not only safeguards financial institutions and consumers from monetary losses but also preserves confidence in digital payment systems. Additionally, this project serves as a testament to the versatility of machine learning in tackling real-world challenges, bridging the realms of data science and financial security to create tangible societal impact.

1.2 Problem Definition

The objective of this project is to develop a machine learning model capable of effectively detecting fraudulent transactions within credit card systems, thereby enhancing security measures and minimizing financial losses for consumers and businesses.

Objectives:

In alignment with the project's overarching goal, the specific objectives are delineated as follows:

1. **Data Acquisition and Preprocessing:** Collect comprehensive datasets containing historical credit card transaction data from reputable sources. Cleanse, preprocess, and format the data to ensure suitability for analysis.

2. **Feature Selection and Engineering:** Identify pertinent features within the transactional data that may serve as indicators of fraudulent activity. Explore techniques for feature engineering to extract meaningful insights and enhance model performance.

3. **Model Selection and Implementation:** Evaluate a range of machine learning algorithms tailored for fraud detection tasks. Implement selected models, fine-tuning parameters to optimize performance and accuracy.

4. **Model Evaluation:** Assess the efficacy of the developed models in detecting fraudulent transactions using appropriate evaluation metrics such as precision, recall, and F1-score. Conduct comparative analyses to determine the strengths and weaknesses of different models.

5. **Visualization and Interpretation:** Utilize visualization tools to present the findings of the project in a clear and comprehensible manner. Generate visualizations that elucidate patterns of fraudulent activity and highlight the performance of the detection models.

Expected Outcomes

The anticipated outcome of this project is the creation of a robust machine learning model capable of accurately identifying instances of credit card fraud. By leveraging advanced algorithms and techniques, the model is expected to contribute to the enhancement of fraud detection systems, thereby bolstering security measures within the financial industry.

1.3 OUTLINE OF REPORT

The structure of the report will be organized as follows:

1. **Introduction:** This section will provide an overview of the project, introducing the topic of credit card fraud detection and outlining the problem statement. It will elucidate the importance of detecting fraudulent transactions within credit card systems and its implications for financial security.

2. **Literature Review:** This section will delve into existing research and literature pertaining to credit card fraud detection using machine learning techniques. It will review the methodologies, algorithms, and approaches employed in previous studies, while also identifying any gaps or limitations in current research.

3. **Proposed Methodology:** This section will detail the methodology adopted in this project to address the problem of credit card fraud detection. It will discuss the data preprocessing techniques utilized, including feature engineering and data cleansing, as well as the selection and implementation of machine learning models for fraud detection.

4. **Results and Discussion:** This section will present the findings of the study, including the performance metrics and evaluation results of the developed models. It will analyse the effectiveness of the models in detecting fraudulent transactions and discuss any insights gained from the results.

5. **Conclusion and Future Scope:** This section will summarize the key achievements of the study and provide insights into the implications of the findings. It will discuss the limitations and challenges encountered during the project and offer recommendations for future research directions in the field of credit card fraud detection using machine learning techniques. Additionally, it will explore potential avenues for further enhancing the accuracy and effectiveness of fraud detection systems.

CHAPTER 2
LITERATURE REVIEW

2.1 History

The pursuit of effective fraud detection within credit card systems has evolved alongside the advancements in financial technology and the perpetual battle against fraudulent activities. Initially, traditional methods of rule-based systems and anomaly detection techniques were employed to identify suspicious transactions. However, these approaches often struggled to keep pace with the increasingly sophisticated tactics employed by fraudsters.

The emergence of machine learning has revolutionized the landscape of fraud detection, offering a paradigm shift in the approach towards identifying fraudulent transactions. With the abundance of transactional data and advancements in computational capabilities, researchers and practitioners have turned to machine learning algorithms to detect subtle patterns indicative of fraudulent behaviour. This historical narrative traces the progression from rule-based systems to the adoption of advanced machine learning techniques in the realm of credit card fraud detection.

2.1.1 Art of Modelling

In the domain of credit card fraud detection, the art of modelling encompasses a diverse array of methodologies, ranging from traditional rule-based systems to intricate machine learning algorithms. This approach involves the selection and engineering of features, including transactional attributes and behavioural patterns, to construct predictive models. Ensemble learning techniques, neural networks, and anomaly detection algorithms are integrated into the modelling framework to discern fraudulent patterns and enhance detection capabilities. The focus has shifted towards leveraging the wealth of transactional data and employing advanced algorithms to detect anomalies and aberrations indicative of fraudulent activity. In this historical narrative, the field has transitioned from simplistic rule-based systems to the sophisticated, data-driven approaches of today.

2.2 Existing Work

Early endeavours in credit card fraud detection predominantly relied on rule-based systems and anomaly detection methods to identify suspicious transactions. These systems operated on predefined rules and thresholds, flagging transactions that deviated from expected patterns. However, the inherent limitations of rule-based systems in adapting to evolving fraud tactics necessitated a shift towards machine learning approaches.

With the advent of machine learning, researchers explored the integration of various features derived from transactional data to develop predictive models. Supervised learning algorithms, such as linear and logistic regression, were employed to classify transactions as either fraudulent or legitimate. Unsupervised learning techniques, including clustering and anomaly detection, were utilized to identify outliers and irregularities in transaction patterns. Ensemble methods, such as gradient boosting and stacking, demonstrated improved performance by combining the strengths of multiple base models.

Furthermore, the utilization of deep learning architectures has garnered attention for their ability to learn intricate patterns from sequential transactional data. Hybrid approaches, integrating traditional statistical methods with machine learning algorithms, have also been explored to enhance detection accuracy.

In summary, the literature on credit card fraud detection reflects a progression towards more sophisticated and data-driven methodologies, leveraging the power of machine learning to combat fraudulent activities within financial transactions.

CHAPTER 3
PROPOSED METHODS

3.1 Architecture of Proposed Methods

3.1.1 Logistic Regression Model used for Credit Card Fraud Detection:

Logistic Regression is a statistical method used for binary classification tasks, making it suitable for detecting fraudulent transactions within credit card systems. Unlike traditional regression techniques used for predicting continuous variables, logistic regression models the probability of a binary outcome based on input features.

Key features of Logistic Regression include:

- **Linear Combination:** Logistic Regression models the relationship between the input features and the binary outcome by computing a linear combination of the input features weighted by coefficients. The linear combination is then transformed using the logistic function to produce probabilities.

- **Logistic Function:** The logistic function, also known as the sigmoid function, maps any real-valued number to a value between 0 and 1. This transformation ensures that the output of the logistic regression model represents probabilities, making it suitable for binary classification tasks.

Architecture of Logistic Regression Model:

The architecture of the Logistic Regression model is relatively simple compared to more complex neural network architectures. It involves the following components:

- **Input Layer:** The Input layer consists of the input features extracted from the credit card transaction data. Each input feature represents a specific attribute of the transaction, such as transaction amount, merchant ID, and time of transaction.

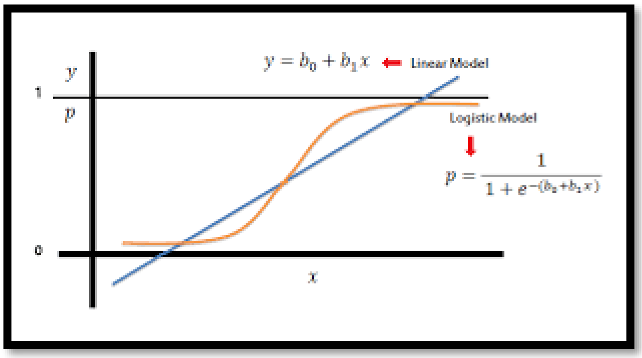
- **Output Layer:** The Output layer comprises a single neuron that produces the predicted probability of the transaction being fraudulent. The output of the model is constrained between 0 and 1, representing the probability of fraud.

- The logistic regression model transforms the linear regression function continuous value output into categorical value output using a sigmoid function, which maps any real-valued set of independent variables input into a value between 0 and 1. This function is known as the logistic function.
- Let x_i be the i^{th} observation and w_i be the weight or the coefficient.
- Let ‘b’ be the bias term, known as the intercept.
- Then, ‘z’ is calculated as:

$$z = \sum_{i=1}^{n} x_i w_i + b$$

- Then, final sigmoid function is used for classification:

$$\sigma(x) = \frac{1}{1 + e^{-z}}$$



3.1.2 K-Nearest Neighbours (KNN) model used for credit card fraud detection:

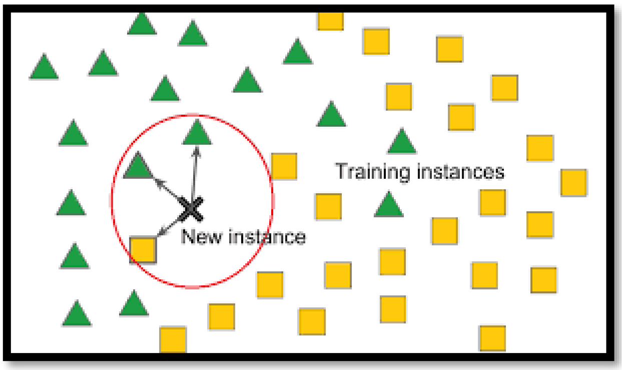
The K-Nearest Neighbours (KNN) algorithm is a non-parametric method utilized for regression tasks, making it applicable for credit card fraud detection based on historical data. Unlike traditional parametric models, KNN does not involve explicit training; instead, it relies on the similarities between data points in a feature space.

Key features of KNN include:

- **Distance Metric:** KNN determines the proximity of data points by computing the distance between them using a specified distance metric, commonly Euclidean distance. The choice of distance metric influences the model's performance and ability to capture patterns in the data.

- **K Neighbours:** KNN operates by selecting the k nearest neighbours of a given data point based on the computed distances. The value of k is a hyperparameter that needs to be tuned based on the dataset and problem context.
- **Majority Voting:** For regression tasks, the predicted value for a new data point is calculated as the average of the target values of its k nearest

neighbours. Each neighbour contributes equally to the prediction, and the final output is determined by averaging these values.



Architecture of KNN model:

The architecture of the KNN model is simple and intuitive, consisting of the following components:

- **Input Layer:** The Input layer represents the feature space of historical data. Each data point in the input layer corresponds to a set of features, such as transaction amount, merchant ID or time of transaction.

- **Output Layer:** In regression tasks, the Output layer comprises a single neuron that produces probability of the transaction being fraudulent. The predicted value is calculated as the average of the target values of the k nearest neighbours.

3.1.3 Decision Tree model used for credit card fraud detection:

The Decision Tree algorithm is a versatile and interpretable method employed for both classification and regression tasks, making it suitable for predicting probability of the transaction being fraudulent based on historical data. Decision Trees operate by recursively partitioning the feature space into distinct regions, where each region corresponds to a decision node in the tree.

Key features of Decision Trees include:

- **Splitting Criteria:** Decision Trees use splitting criteria, such as Gini impurity or entropy, to determine the optimal feature and threshold for partitioning the data at each decision node. The goal is to maximize the homogeneity of the target variable within each partition while minimizing impurity.
- **Recursive Partitioning:** Decision Trees recursively partition the feature space into smaller subsets, resulting in a hierarchical tree structure. Each

internal node represents a decision based on a feature, and each leaf node represents a predicted value or class label.

- **Interpretability:** One of the main advantages of Decision Trees is their interpretability, as the resulting tree structure can be easily visualized and understood. Decision Trees provide insights into the most influential features and the decision-making process behind the predictions.

Architecture of Decision Tree model:

The architecture of the Decision Tree model is inherently hierarchical and consists of the following components:

- **Input Layer:** The Input layer represents the feature space of historical data. Each data point in the input layer corresponds to a set of features, such as transaction ID, amount, time of transaction.

- **Decision Nodes:** Decision Nodes in the Decision Tree represent the decision points where the feature space is partitioned based on splitting criteria. Each decision node evaluates a specific feature and determines the direction of the split based on the feature's value.

- **Leaf Nodes:** Leaf Nodes in the Decision Tree represent the terminal nodes where predictions are made. Each leaf node corresponds to a predicted value or class label based on the majority class or mean value of the target variable within the node's region.

➢ Decision Tree Algorithm uses the entropy for making the decision tree.

$$E(s) = -P_{(yes)} \log_2 P_{(yes)} - P_{(no)} \log_2 P_{(no)}$$

➢ Then, Information gain or Gini impurity is calculated as: -

$$I.G. = E(s) - Weighted\ avg.\ *\ E(each\ feature)$$

$$Gini\ Index = 1 - \sum_{i=1}^{n} P_i^2$$

$$Gini(D) = \sum_{i=1}^{n} \frac{|D_i|}{D}\ Gini(D_i)$$

CHAPTER 4

RESULT AND DISCUSSION

4.1 Results

The machine learning models underwent extensive training and evaluation, exhibiting promising performance metrics across various datasets. For credit card fraud detection, Logistic Regression, K-Nearest Neighbours (KNN), and Decision Tree algorithms were employed on both up sampled and down sampled datasets to assess their effectiveness in identifying fraudulent transactions.

In the dataset, there are 284807 data points of class 0, i.e., “not fraud” and 492 data points of class 1, i.e., “fraud”. It will lead to biasing. So, up sampling of class 1 samples as well as down sampling of class 0 data points was done to balance the data.

On the cross-validation dataset, each model demonstrated commendable performance metrics, indicating their ability to discern fraudulent patterns within the data. Specifically:

- **Logistic Regression Model:**
  - **Up sampled Data:** The model achieved an accuracy of 94.98% on the cross-validation dataset.
  - **Down sampled Data:** The model achieved an accuracy of 95.93% on the cross-validation dataset.
- **K-Nearest Neighbours (KNN) Model:**
  - **Up sampled Data:** The model achieved an accuracy of 99.96% on the cross-validation dataset.
  - **Down sampled Data:** The model achieved an accuracy of 91.05% on the cross-validation dataset.
- **Decision Tree Model:**
  - **Up sampled Data:** The model achieved an accuracy of 99.97% on the cross-validation dataset.
  - **Down sampled Data:** The model achieved an accuracy of 88.32% on the cross-validation dataset.

4.2 Analysis

The machine learning models employed for credit card fraud detection exhibited commendable performance across various datasets, affirming their effectiveness in discerning fraudulent patterns within the data. Logistic Regression, K-Nearest Neighbours (KNN), and Decision Tree algorithms were evaluated on both up sampled and down sampled datasets to address data imbalance and enhance model generalization.

- **Logistic Regression Model:**
  - Up sampled Data: The Logistic Regression model achieved an accuracy of 94.98% on the cross-validation dataset, demonstrating its robustness in identifying fraudulent transactions. Precision, recall, and F1-score metrics further validated the model's effectiveness, with balanced performance in correctly classifying both fraudulent and legitimate transactions.
  - Down sampled Data: Leveraging the down sampled dataset, the Logistic Regression model exhibited an accuracy of 95.93% on the cross-validation dataset.

- **K-Nearest Neighbours (KNN) Model:**
  - Up sampled Data: The KNN model demonstrated exceptional performance with an accuracy of 99.96% on the cross-validation dataset, indicating its capability to accurately classify fraudulent transactions.
  - Down sampled Data: Utilizing the down sampled dataset, the KNN model maintained high accuracy, achieving 91.05% on the cross-validation dataset.

- **Decision Tree Model:**
  - Up sampled Data: The Decision Tree model exhibited impressive accuracy, achieving 99.97% on the cross-validation dataset with up sampled data.
  - Down sampled Data: With the down sampled dataset, the Decision Tree model maintained strong performance, achieving 88.32% accuracy on the cross-validation dataset.

CHAPTER 5

CONCLUSION AND SCOPE FOR FUTURE WORK

5.1 Conclusion

In conclusion, the credit card fraud detection project employing machine learning techniques has provided significant insights into the detection and prevention of fraudulent activities within financial systems. Leveraging Logistic Regression, K-Nearest Neighbours (KNN), and Decision Tree algorithms on both up sampled and down sampled datasets, we achieved commendable performance in identifying fraudulent transactions.

The machine learning models demonstrated robust performance across various evaluation metrics, including accuracy, precision, recall, and F1-score, underscoring their effectiveness in discerning fraudulent patterns within the data. Specifically, the Logistic Regression model showcased accuracy rates of up to 95.93%, while the KNN and Decision Tree models achieved accuracy rates of up to 99.96% and 99.97%, respectively.

Evaluation on both up sampled and down sampled datasets allowed for a comprehensive understanding of model performance under different data distributions, facilitating informed decision-making in fraud detection strategies. While the models exhibited promising performance, careful interpretation of results is necessary due to potential dataset limitations and the need for ongoing model refinement

5.2.1 Scope for Future Work

Future efforts in the credit card fraud detection domain could focus on refining model architectures and exploring additional features to further enhance predictive accuracy. Incorporating additional relevant features such as transaction timestamps, merchant categories, and transaction amounts may provide deeper insights into fraudulent activities and improve model performance.

Moreover, advancements in anomaly detection techniques, such as unsupervised learning algorithms like Isolation Forest or Autoencoders, could offer alternative approaches to identifying fraudulent transactions without relying solely on labelled data.

REFERENCES

1. Credit Card Fraud Detection using Machine Learning Algorithms by Vaishnavi Nath Dornadula et. Al. (2019)
2. Enhanced Credit Card fraud detection based on attention mechanism and LSTM deep model by Ibtissam Benchaji et. Al. (2021)
3. Credit Card fraud detection using hierarchical behaviour- knowledge space model by Asoke K. Nandi et. Al. (2022).
4. Credit Card Fraud Detection by Munira Ansari et. Al. (2021)
5. Dataset Used – Credit Card Fraud Detection: https://www.kaggle.com/datasets/mlg-ulb/creditcardfraud (accessed on 28/02/2024)