

Detecting Sophisticated Frauds in Online Payments using Machine Learning

**A PROJECT REPORT
SUBMITTED IN PARTIAL FULFILLMENT OF THE
REQUIREMENTS FOR THE COMPLETION OF
CS4200-MAJOR PROJECT**

**BACHELOR OF TECHNOLOGY
IN
COMPUTER SCIENCE AND ENGINEERING**

SUBMITTED BY

**M.Shiva Keshava Reddy
(Enrollment No. 21CS002396)**



**FACULTY OF COMPUTING AND INFORMATICS
SIR PADAMPAT SINGHANIA UNIVERSITY
UDAIPUR 313601, INDIA**

JAN, 2025

Detecting Sophisticated Frauds in Online Payments using Machine Learning

*a Project Report
Submitted in partial fulfillment of the requirements
for CS4200-Major Project*

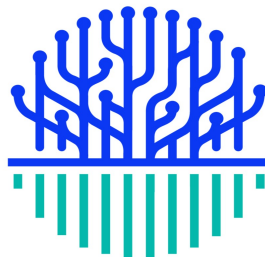
BACHELOR OF TECHNOLOGY
in
Computer Science & Engineering

submitted by

M.Shiva Keshava Reddy
(Enrollment No. 21CS002396)

Under the guidance of
Prof. Alok Kumar
(Project Coordinator)

and
Dr. Gurpreet Singh
(Supervisor)



FACULTY OF COMPUTING AND INFORMATICS
SIR PADAMPAT SINGHANIA UNIVERSITY
UDAIPUR 313601, India

JAN, 2025



**Faculty of Computing and Informatics
Sir Padampat Singhania University
Udaipur, 313601, India**

CERTIFICATE

I, **M.Shiva Keshava Reddy**, hereby declare that the work presented in this project report entitled “**Detecting Sophisticated Frauds in Online Payments using Machine Learning**” for the completion of CS4200-Major Project and submitted in the **Faculty of Computing and Informatics** of the **Sir Padampat Singhania University, Udaipur** is an authentic record of my own work carried out under the supervision of **Prof. Alok Kumar, Professor**, and **Dr. Gurpreet Singh, Assistant Professor**. The work presented in this report has not been submitted by me anywhere else.

M.Shiva Keshava Reddy
(21CS002396)

This is to certify that the above statement made by the candidate is true to the best of my knowledge and belief.

Prof. Alok Kumar
Professor
Project Coordinator

Dr. Gurpreet Singh
Assistant Professor
Supervisor

Place: Udaipur
Date:

Acknowledgements

Inscribing these words of gratitude feels akin to painting a masterpiece on the canvas of appreciation. This incredible path of learning and exploration would not have been possible without the unflinching support and encouragement of the great individuals who have paved the road for my accomplishment.

I reserve a special place in my heart for my beloved parents, whose unwavering love, unwavering support, and unwavering belief in my abilities have been the bedrock upon which my dreams have flourished. Their persistent support, sacrifices, and unshakable trust in my abilities have been the driving factors behind my quest for knowledge and academic pursuits.

First and foremost, I owe a tremendous debt of gratitude to my esteemed supervisor, **Dr.Gurpreet Singh** , whose guidance and advice have been the compass guiding me through the many twists and turns of this thesis. His stimulating conversations, insightful feedback, kind advice, and boundless forbearance have challenged me to push the boundaries of my capabilities and inspired me to strive for academic excellence. I am very thankful for the trust you put in me and the chances you gave me to grow both professionally and personally. I am grateful beyond words for the opportunity to have worked under your guidance, and I hope my thesis serves as a fitting tribute to your hard work, knowledge, and encouragement.

I like to thank **Dr.Alok Kumar** , Professor, Computer Science and Engineering Department, and **Dr.Chandrashekhar Goswami** , Head of the Department, Computer Science and Engineering Department, for their extended support.

I would like to extend a heartfelt thank you to, **Mr.Sharath** , **Mr. Kalyan**, **Mr. Deepak**, **Mr. Jeethu**, **Mr. Rakesh** my incredible classmates and friends, who have been a constant source of support, camaraderie, and inspiration. Their presence has made the often-trying process of writing a thesis into one that is filled with joy and fun. Finally, I want to thank everyone who helped me grow as a scholar and made this trip unforgettable.

M.Shiva Keshava Reddy

Abstract

The study titled "Detecting Sophisticated Frauds in Online Payments using Machine Learning" addresses the critical challenge of identifying and preventing online payment fraud, a growing concern in the rapidly expanding e-commerce landscape. As digital transactions become increasingly prevalent, so too do the sophisticated tactics employed by fraudsters, necessitating the development of advanced detection mechanisms that can operate in real-time to protect both businesses and consumers.

This research focuses on creating a robust fraud detection system that leverages machine learning algorithms to analyze a wide array of data, including transactional records, user behavior patterns, and contextual information surrounding each transaction. By employing techniques such as data preprocessing and feature engineering, the system aims to extract relevant features that can effectively distinguish between legitimate and fraudulent transactions. Various machine learning models are utilized in this study, including logistic regression, random forest, and neural networks, each chosen for their unique strengths in handling complex data patterns.

One of the key innovations of this system is its ability to perform real-time detection of suspicious transactions. This capability is crucial for minimizing potential losses, as it allows for immediate intervention when fraud is suspected. Additionally, the system incorporates continuous learning mechanisms that enable it to adapt to emerging fraud tactics over time. This adaptability is further enhanced by integrating behavioral biometrics, which analyze user-specific behaviors—such as typing speed or mouse movements—to improve detection accuracy.

To evaluate the effectiveness of the proposed models, the research employs various performance metrics, including precision, recall, and F1-score. These metrics help ensure that the system not only identifies fraudulent transactions accurately but also minimizes false positives, which can lead to unnecessary disruptions for legitimate users.

In conclusion, this research makes a significant contribution to the field of online payment security by providing a comprehensive solution for fraud detection. By harnessing the power of machine learning, the system enhances detection capabilities while fostering greater trust in digital payment environments. Ultimately, this work aims to protect businesses and consumers from the financial losses associated with online fraud, paving the way for safer e-commerce practices.

Contents

Certificate	ii
Acknowledgements	iii
Abstract	iv
Contents	v
List of Figures	vii
List of Tables	viii
List of Abbreviations	ix
1 Introduction	1
1.1 Motivation	2
1.2 Purpose of the System	2
1.2.1 Scope of the Project	2
1.3 Problem Statement & Objectives	2
1.3.1 Problem Statement	2
A. Increasing Sophistication of Fraud Techniques	2
B. Limitations of Traditional Detection Methods	3
C. Data Complexity and Volume	3
D. Regulatory and Compliance Challenges	3
E. The Role of Machine Learning	3
1.3.2 Objectives	3
1.4 Structure of the Dissertation	4
2 Literature Review	5
2.1 literature survey	5
2.1.1 Fraud Detection Frameworks in Online Payments:	5
A. Traditional Approaches:	5
2.2 Table	6
A. Machine Learning Approaches:	6
2.2.1 Machine Learning Algorithms for Fraud Detection:	7
A. Supervised Learning Algorithms:	7
B. Unsupervised Learning Algorithms:	7
C. Feature Engineering and Data Representation:	7
D. Addressing Class Imbalance:	8
E. Evaluation Metrics:	8
F. Challenges and Opportunities:	8
G. Recent Advances and Emerging Trends:	8
2.2.2 Feasibility Study	9
A. Economic Feasibility	9
B. Technical Feasibility	9

C.	Social Feasibility	9
3	Methodology	11
3.1	Problem Formulation	11
3.2	Data	12
3.2.1	step	12
3.2.2	type	12
3.2.3	amount	12
3.2.4	Name Orig	12
3.2.5	Old balance Orig	12
3.2.6	New balance Orig	12
3.2.7	Name Dest	12
3.2.8	Old balance Dest	12
3.2.9	New balance Dest	13
3.2.10	Is Fraud	13
3.2.11	Is Flagged Fraud	13
3.3	Data preprocessing:	13
3.4	Feature selection:	15
3.5	Model training	15
3.6	Machine learning algorithms	15
3.6.1	Decision Tree	15
3.6.2	Logistic Regression	15
3.6.3	Navie Bayes Classifier	15
	A. Bayes Theorem:	16
3.7	Model Architecture	16
3.8	Model evaluation	17
3.9	Model selection	17
3.10	Hyperparameter tuning	17
4	Results and Discussion	19
5	Conclusions and Future Scope	21
5.1	Conclusions	21
5.2	Future Scope	22
	List of Publications	23
	References	23

List of Figures

3.1	Data collection	13
3.2	Distribution pie chart	14
3.3	Decision Tree	16
3.4	architecture	17
4.1	Differentiation between fraud or notfraud	20

List of Tables

2.1	Methods and its Limitations	6
-----	---------------------------------------	---

List of Abbreviations

CNN	Convolutional Neural Networks
RNN	Recurrent Neural Networks
GBM	Gradient Boosting Machines
SMOTE	Since fraudulent transactions are rare, techniques like oversampling
SVM	Support vector machines

Chapter 1

Introduction

The increasing availability of online payment methods and the growth of e-commerce have led to a notable increase in fraudulent activity. Reliable sources show that between 2020 and 2022, there will be a sharp and sudden rise in the amount of money lost to credit and debit card theft. Both government agencies and private companies have significantly raised their spending for RD initiatives in response to these serious issues. Their main goal is to develop more robust and efficient techniques for identifying fraudulent activity. Financial institutions that control online transaction processing and credit card issuing must now install automated fraud detection systems. These solutions are essential for increasing consumer confidence and trust in addition to helping to minimize financial losses. Emerging opportunities in the fields of artificial intelligence and big data have emerged, offering fascinating prospects, especially when it comes to applying potent machine learning algorithms to the fight against financial crime. With the help of state-of-the-art machine/deep learning algorithms and data analysis, modern fraud detection systems have proven extremely successful.

These algorithms can distinguish between legitimate and fraudulent activities since they are typically trained on big datasets of labelled transactions. The creation of binary classification models with the ability to differentiate between legitimate and fraudulent transactions is the final outcome. Using classification algorithms to detect fraudulent transactions is a challenging attempt that calls for present creativity and adaptability. The financial sector needs to develop constantly to remain ahead of financial crime in the same manner that innovation ensures security, data availability, reliability, and resilience against cyberwarfare assaults in the fight against wireless communication interference.

[1]

1.1 Motivation

The motivation for online transaction lies in the desire to identify and address the risk of fraud. By leveraging predictive analytics and machine learning techniques, organizations can gain insights from historical data to understand the factors contributing to fraud payments. This empowers them to minimize false positives, enhance the customer experience, and ensure compliance with regulatory requirements. Predictive models enable early identification of fraud transactions. Ultimately, the motivation is to optimize fraud transactions, enhance customer satisfaction, and ensure the long-term success of the organization.

1.2 Purpose of the System

Online payment fraud detection in a proposed system involves leveraging data-driven techniques, that are used to identify and prevent fraudulent transactions in real-time. By analyzing historical data, factors like amount, old balance, new balance can be considered. Utilizing machine learning algorithms, such as logistic regression or decision trees, can aid in creating predictive models. Regularly monitoring these models and identifying early warning signs can help, to adapt evolving fraud threats, minimize false positives, enhance the customer experience, and ensure compliance with regulatory requirements.

1.2.1 Scope of the Project

The scope of the project encompasses the development and implementation of a online payment fraud detection model, utilizing data analysis and machine learning to forecast whether the transaction is fraud (or) not.

1.3 Problem Statement & Objectives

1.3.1 Problem Statement

The problem state of detecting sophisticated frauds in online payments using machine learning encompasses several critical challenges that have emerged due to the evolving landscape of digital transactions. As online payment systems continue to grow in popularity, the associated risks and complexities of fraud detection have also intensified.

A. Increasing Sophistication of Fraud Techniques

Fraudsters are becoming increasingly adept at circumventing traditional security measures. They exploit vulnerabilities in online payment systems, leveraging advanced technologies and methodologies to conduct unauthorized transactions. The rise of a cyber-crime ecosystem, complete with tools and services for fraud, has made it easier for attackers to develop and implement sophisticated strategies that challenge existing detection mechanisms . This cat-and-mouse game between fraudsters and businesses necessitates continuous innovation in fraud detection technologies. [2]

B. Limitations of Traditional Detection Methods

Traditional fraud detection methods often rely on static rules and thresholds that can be easily bypassed by skilled attackers. These systems may flag legitimate transactions as fraudulent, leading to high false positive rates that frustrate customers and damage business reputations. Moreover, the lack of adaptability in these systems means they struggle to recognize new patterns of fraudulent behavior, resulting in missed opportunities to prevent fraud [1][3]. As such, there is a pressing need for more dynamic and intelligent solutions.

C. Data Complexity and Volume

The sheer volume and complexity of transaction data present another significant challenge. Online payment systems generate vast amounts of data daily, including user behaviors, transaction histories, and contextual information. Analyzing this data effectively requires advanced machine learning algorithms capable of processing unstructured data and identifying subtle patterns indicative of fraud [2][3]. However, developing models that can accurately learn from such diverse datasets while minimizing errors remains a complex task.

D. Regulatory and Compliance Challenges

The regulatory landscape surrounding online payments is often fragmented, with varying compliance requirements across different regions. This inconsistency complicates the enforcement of uniform security standards, creating loopholes that fraudsters can exploit [1]. Additionally, weak authentication methods—such as poor password practices—further exacerbate the problem by providing easy access points for attackers .

E. The Role of Machine Learning

Machine learning offers a promising avenue for addressing these challenges by enabling real-time analysis of transaction data to detect anomalies. By employing algorithms that learn from historical data, businesses can enhance their ability to identify fraudulent activities with greater accuracy and speed [3][4]. However, implementing machine learning solutions requires significant investment in technology and expertise, which may not be feasible for all organizations.

In summary, the problem state of detecting sophisticated frauds in online payments using machine learning is characterized by the increasing sophistication of fraud techniques, limitations of traditional detection methods, complexities associated with large volumes of data, regulatory challenges, and the potential benefits offered by machine learning technologies. Addressing these issues is crucial for businesses aiming to protect themselves and their customers from the growing threat of online payment fraud. As the digital payment landscape continues to evolve, ongoing research and development in machine learning applications will be essential for staying ahead of fraudulent activities.

1.3.2 Objectives

- (i) **Real-Time Fraud Detection:** Develop a robust system capable of identifying and flagging fraudulent transactions in real-time by analyzing transactional data and user behavior patterns.

- (ii) **Utilization of Machine Learning Algorithms:** Employ various machine learning techniques, such as logistic regression, random forest, and neural networks, to effectively recognize anomalies indicative of fraudulent activities.
- (iii) **Data Preprocessing and Feature Engineering:** Implement data preprocessing and feature engineering strategies to enhance the quality of input data, improving the overall performance and accuracy of the fraud detection models.
- (iv) **Performance Evaluation:** Assess the effectiveness of the developed system using metrics like precision, recall, and F1-score to ensure a balance between accurately detecting fraud and minimizing false positives, thereby fostering trust in online payment systems.

1.4 Structure of the Dissertation

Detecting sophisticated frauds in online payments using machine learning presents several limitations that can hinder the effectiveness of fraud detection systems. One significant challenge is the requirement for large volumes of high-quality data; machine learning algorithms rely heavily on comprehensive datasets to train effectively. If the data is biased, incomplete, or lacks sufficient detail, the algorithms may produce inaccurate predictions, leading to missed fraudulent activities or false positives that can frustrate legitimate users. Additionally, many machine learning models operate as "black boxes," making it difficult for stakeholders to interpret their decisions and understand why certain transactions are flagged as suspicious. This lack of transparency can undermine trust in the system and complicate compliance with regulatory requirements. Moreover, the dynamic nature of fraud poses a persistent challenge, as fraudsters continually adapt their tactics to evade detection. This necessitates ongoing updates and retraining of models, which can be resource-intensive and costly for organizations. Furthermore, the issue of data imbalance arises since fraudulent transactions are typically much rarer than legitimate ones. This imbalance can skew model training, resulting in systems that are less effective at identifying fraudulent activities. Finally, ensuring data privacy and security is paramount; handling sensitive financial information requires strict adherence to regulations, adding another layer of complexity to the implementation of machine learning-based fraud detection systems. These limitations highlight the need for continuous improvement and adaptation in fraud detection methodologies to effectively combat evolving threats in online payment systems. [3]

Chapter 2

Literature Review

2.1 literature survey

Online payment systems have become an essential part of the modern economy, but with their growth, there has been a significant rise in fraudulent activities. Fraudulent transactions can cause severe financial losses and undermine the integrity of online payment systems. Detecting frauds in real-time has thus become a major challenge. Machine Learning (ML) techniques have emerged as effective tools for identifying fraudulent activities, even those that are sophisticated and hard to detect with traditional methods.

2.1.1 Fraud Detection Frameworks in Online Payments:

Fraud detection generally revolves around identifying abnormal patterns in transaction data. Several frameworks have been proposed for detecting frauds, including rule-based systems, statistical models, and machine learning algorithms. Traditionally, rule-based systems were employed, where specific fraud scenarios were predefined. However, these systems struggle with complex or adaptive fraud schemes, as they cannot identify new or unforeseen fraudulent behaviors.

A. Traditional Approaches:

Rule-based systems: rely on predefined patterns and thresholds to flag transactions as fraudulent.

Statistical methods (like logistic regression or decision trees) are often employed to predict the likelihood of fraud based on historical transaction data.

2.2 Table

Methods	Limitations
SVM	<ul style="list-style-type: none">• Requires large labeled datasets, which may be difficult to obtain.• Fraud cases are rare, leading to model bias.
Anomaly Detection	<ul style="list-style-type: none">• High rate of legitimate transactions flagged as fraudulent.• Defining "normal" behavior can be difficult, leading to false negatives.
Unsupervised Learning	<ul style="list-style-type: none">• Fraud might not be clearly identified without manual intervention.• High computational cost for large datasets with many features.
Ensemble Methods	<ul style="list-style-type: none">• Combining multiple models can complicate the system and make it harder to interpret.• Ensemble methods can still suffer from overfitting if not tuned properly.
Deep Learning Neural Networks	<ul style="list-style-type: none">• Requires vast amounts of data for effective training.• Difficult to interpret, leading to challenges in trust and transparency.

Table 2.1: Methods and its Limitations

A. Machine Learning Approaches:

Machine learning techniques, especially supervised and unsupervised learning, have become more popular due to their ability to handle large and complex datasets and identify hidden patterns.

2.2.1 Machine Learning Algorithms for Fraud Detection:

Several ML techniques are widely used for detecting fraud in online payments. Some of the prominent ones include:

A. Supervised Learning Algorithms:

Logistic Regression is a simple yet effective technique commonly used for binary classification problems, such as distinguishing between fraud and non-fraudulent transactions. It provides a straightforward approach to model the relationship between features and the outcome. Ensemble models like Random Forest and Decision Trees are also widely used in fraud detection, as they are effective at capturing non-linear relationships in the data, enabling them to handle complex interactions between features. Support Vector Machines (SVM) are known for their ability to work well in high-dimensional spaces, making them particularly useful for fraud detection tasks that involve many features. SVMs also provide good classification accuracy, especially when dealing with intricate decision boundaries. On the other hand, Neural Networks, particularly deep learning models like Recurrent Neural Networks (RNNs) and Convolutional Neural Networks (CNNs), have shown great promise in analyzing sequential transaction data. These models can capture temporal dependencies and patterns, making them ideal for detecting fraud in transaction sequences where the order and timing of events play a critical role.

B. Unsupervised Learning Algorithms:

Clustering algorithms like K-Means and DBSCAN are commonly used in fraud detection to identify unusual groups of transactions that may indicate fraudulent activity, even in the absence of labeled data. These unsupervised methods can help discover patterns or clusters in transaction data that differ significantly from normal behavior, which could be indicative of fraud. Anomaly detection algorithms, such as Isolation Forest, One-Class SVM, and Autoencoders, are also popular choices for detecting outliers in transaction data. These models focus on identifying data points that deviate from the norm, as fraud is often represented as such outliers. By detecting these anomalies, the models can flag suspicious activities that may be missed by traditional methods. Hybrid approaches, which combine both supervised and unsupervised techniques, offer an additional layer of sophistication to fraud detection. By combining clustering with classification models, for instance, hybrid models can leverage the strengths of both approaches to improve detection accuracy, capturing both known and unknown fraud patterns while ensuring that false positives are minimized.

C. Feature Engineering and Data Representation:

Effective fraud detection relies on extracting relevant features that can differentiate between fraudulent and legitimate transactions. Key features used in fraud detection include user behavior features like transaction history, frequency of transactions, geographical locations, and devices used. Transaction features such as the transaction amount, time of transaction, payment method, and merchant information are also crucial for detecting anomalies. Additionally, behavioral profiling is important for tracking a user's typical behaviors and flagging deviations, while graph-based features utilize network

analysis to detect relationships between users, devices, and accounts involved in multiple transactions. However, feature engineering faces several challenges, such as missing data, high-dimensionality, and class imbalance where fraudulent transactions are rare. The need for real-time processing also adds complexity, as models must make quick decisions without compromising accuracy.

D. Addressing Class Imbalance:

A significant challenge in fraud detection is class imbalance, where fraudulent transactions are much less frequent than legitimate ones. To address this issue, several strategies are employed. Resampling techniques, such as oversampling the minority class (fraudulent transactions) or undersampling the majority class (legitimate transactions), are used to balance the dataset. Cost-sensitive learning adjusts the cost of misclassifying fraudulent and legitimate transactions, making the model more sensitive to fraud. Anomaly detection is another method, as fraud often appears as outliers in the dataset, requiring the model to identify these rare events.

E. Evaluation Metrics:

To assess the performance of fraud detection systems, various evaluation metrics are used. Accuracy, which measures the proportion of correctly classified transactions, can be misleading in imbalanced datasets. Precision and recall are more important metrics, with precision measuring the correctly identified fraudulent transactions out of all flagged transactions, and recall assessing the model's ability to detect all fraudulent transactions. The F1-score, the harmonic mean of precision and recall, helps balance the two metrics, while the AUC-ROC curve provides a visual representation of the model's ability to distinguish between fraudulent and legitimate transactions.

F. Challenges and Opportunities:

There are several ongoing challenges and opportunities in fraud detection. Evolving fraud techniques make it difficult for static models to detect new forms of fraud, leading to increased interest in adaptive models and online learning approaches, which can learn incrementally as new data becomes available. Data privacy and security are also major concerns, especially since online payment systems handle sensitive financial data. Techniques like federated learning allow for collaborative training of models without exposing raw data, addressing privacy issues. Additionally, the explainability of models is an important issue, particularly for complex machine learning models like deep learning, as businesses and regulators may require more transparent and understandable models to trust the system.

G. Recent Advances and Emerging Trends:

Recent advances in fraud detection have led to the increased use of deep learning models, particularly Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs), which are effective at identifying complex patterns in transaction data, such as sequence-based patterns and temporal dependencies. Transfer learning has become a valuable tool, enabling pre-trained models to be fine-tuned for fraud detection tasks, thus improving accuracy and reducing training time. Graph-based techniques have gained

popularity, as fraudsters may coordinate their actions across multiple entities. By analyzing relationships between users, devices, and transactions, graph-based models help detect such coordinated fraud. Another promising trend is federated learning, which enables multiple parties to train machine learning models collaboratively while keeping raw data decentralized, helping to address privacy concerns.

Detecting sophisticated fraud in online payments through machine learning is a rapidly evolving field, with ongoing developments in models, techniques, and frameworks. The combination of deep learning, anomaly detection, and feature engineering shows great promise in enhancing fraud detection systems. However, challenges such as class imbalance, evolving fraud tactics, and the need for real-time detection remain obstacles. Moving forward, research will likely focus on developing more robust, scalable, and interpretable models, while improving the integration of machine learning systems into real-world payment infrastructure. With continued advancements, machine learning will play an increasingly vital role in mitigating fraud risks and securing online transactions.

2.2.2 Feasibility Study

The feasibility of the project is analyzed in this phase and business proposal is put forth with a very general plan for the project and some cost estimates. During system analysis the feasibility study of the proposed system is to be carried out. This is to ensure that the proposed system is not a burden to the company. For feasibility analysis, some understanding of the major requirements for the system is essential.

Three key considerations involved in the feasibility analysis are

A. Economic Feasibility

This study is carried out to check the economic impact that the system will have on the organization. The amount of fund that the company can pour into the research and development of the system is limited. The expenditures must be justified. Thus the developed system as well within the budget and this was achieved because most of the technologies used are freely available. Only the customized products had to be purchased.

B. Technical Feasibility

This study is carried out to check the technical feasibility, that is, the technical requirements of the system. Any system developed must not have a high demand on the available technical resources. This will lead to high demands on the available technical resources. This will lead to high demands being placed on the client. The developed system must have a modest requirement, as only minimal or null changes are required for implementing this system.

C. Social Feasibility

The aspect of study is to check the level of acceptance of the system by the user. This includes the process of training the user to use the system efficiently. The user must not feel threatened by the system, instead must accept it as a necessity. The level of

acceptance by the users solely depends on the methods that are employed to educate the user about the system and to make him familiar with it. His level of confidence must be raised so that he is also able to make some constructive criticism, which is welcomed, as he is the final user of the system.

Chapter 3

Methodology

3.1 Problem Formulation

The methodology for detecting sophisticated fraud in online payments using machine learning involves a comprehensive approach that begins with formulating the problem as a binary classification task—distinguishing between fraudulent and legitimate transactions. The first step is data collection, which involves gathering transaction data, user behaviors, payment methods, and device information. Preprocessing this data is crucial to handle missing values, normalize features, and address class imbalance, as fraudulent transactions are far less frequent than legitimate ones. Feature engineering is the next key step, where relevant attributes are extracted from raw transaction data, such as transaction amount, time, user behavior, and device identifiers, to capture potential fraud patterns. The core of the methodology then focuses on applying machine learning algorithms, both supervised and unsupervised, to model the data. Supervised models, such as Logistic Regression, Random Forests, and Support Vector Machines, are trained using labeled data to learn patterns associated with fraud. In contrast, unsupervised techniques, like clustering algorithms (K-Means, DBSCAN) and anomaly detection methods (Isolation Forest, Autoencoders), help detect unknown or novel fraud patterns by identifying outliers in the data. Handling class imbalance is critical, often achieved through techniques like oversampling, undersampling, or cost-sensitive learning, to ensure that fraudulent transactions are appropriately detected. Evaluation metrics such as precision, recall, F1-score, and AUC-ROC curve are used to assess model performance, ensuring a balanced approach to minimizing both false positives and false negatives. Real-time detection capabilities are also incorporated to ensure that fraud can be identified as transactions occur, leveraging low-latency models and incremental learning for continuous adapta-

tion. The model is then deployed and continuously monitored, with periodic retraining to adapt to new fraud tactics. Throughout the process, challenges such as data privacy, model explainability, and the evolving nature of fraud techniques are addressed, ensuring the system remains robust and trustworthy in detecting sophisticated online payment fraud. [4]

3.2 Data

Data collection refers to the process of locating, gathering, and collecting the information needed to create, test, and validate a model. The primary stage of the machine learning process involves gathering data to train the machine learning model. Machine learning (ML) systems can only make predictions with accuracy equal to the quality of the training data. Some of the attributes used in our data set are:

3.2.1 step

Maps a unit of time in the real world. In this case 1 step is 1 hour of time. Total steps 744 (30 days simulation).

3.2.2 type

CASH-IN, CASH-OUT, DEBIT, PAYMENT and TRANSFER.

3.2.3 amount

Amount of the transaction in local currency.

3.2.4 Name Orig

Customer who started the transaction.

3.2.5 Old balance Orig

Initial balance before the transaction.

3.2.6 New balance Orig

New balance after the transaction.

3.2.7 Name Dest

Customer who is the recipient of the transaction.

3.2.8 Old balance Dest

Initial balance recipient before the transaction. Note that there is not information for customers that start with M (Merchants).

3.2.9 New balance Dest

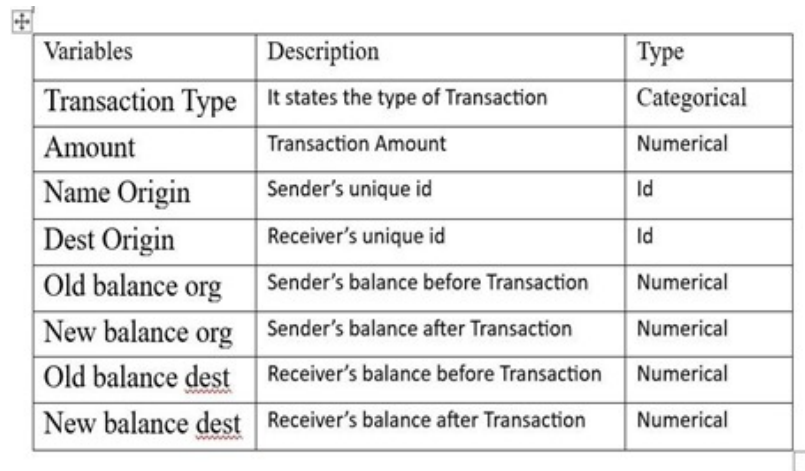
New balance recipient after the transaction. Note that there is not information for customers that start with M (Merchants).

3.2.10 Is Fraud

This is the transactions made by the fraudulent agents inside the simulation. In this specific dataset the fraudulent behavior of the agents aims to profit by taking control or customer's accounts and try to empty the funds by transferring to another account and then cashing out of the system.

3.2.11 Is Flagged Fraud

The business model aims to control massive transfers from one account to another and flags illegal attempts. An illegal attempt in this dataset is an attempt to transfer more than 200.000 in a single transaction.



Variables	Description	Type
Transaction Type	It states the type of Transaction	Categorical
Amount	Transaction Amount	Numerical
Name Origin	Sender's unique id	Id
Dest Origin	Receiver's unique id	Id
Old balance org	Sender's balance before Transaction	Numerical
New balance org	Sender's balance after Transaction	Numerical
Old balance dest	Receiver's balance before Transaction	Numerical
New balance dest	Receiver's balance after Transaction	Numerical

Figure 3.1: Data collection

3.3 Data preprocessing:

Data preprocessing is a crucial step in building an effective fraud detection model for online payments. The raw data, often messy and incomplete, needs to be cleaned and transformed before it can be fed into machine learning algorithms. The first step in preprocessing is data cleaning, which involves handling missing values. This can be done through imputation, where missing values are filled in with the mean, median, or mode of the respective feature, or by removing rows with missing data if they are few. Once the data is cleaned, feature scaling is necessary to standardize the numerical features, especially for algorithms sensitive to feature scales like Support Vector Machines or Neural Networks. Techniques such as normalization (scaling features to a [0, 1] range) or standardization (scaling features to have a mean of 0 and a standard deviation of 1) are commonly used to ensure that all features contribute equally to the model. In addition,

categorical features such as payment methods or merchant IDs must be encoded into numerical values using techniques like one-hot encoding or label encoding.

Handling class imbalance is another important step, as fraudulent transactions are much less frequent than legitimate ones, leading to an imbalanced dataset. This imbalance can be addressed by oversampling the minority class (fraudulent transactions) or undersampling the majority class (legitimate transactions). Another method to address this is through anomaly detection techniques, where fraud is treated as an anomaly or outlier in the dataset. Feature engineering is also essential to improve the model's ability to detect fraud. By creating new features such as transaction amount deviation, frequency of transactions, or the time between transactions, the model can better capture patterns that are indicative of fraudulent behavior. Outliers should be detected and handled, as fraudulent transactions often deviate significantly from normal behavior. Once the data is prepared, it must be split into training and testing sets, typically with 70-80 percent of the data used for training and the remaining 20-30 percent used for testing. Techniques like k-fold cross-validation can also be used to ensure that the model generalizes well and isn't overfitting to a specific subset of the data. In cases where sequence-based models or graph-based models are used, additional preprocessing steps, such as converting data into time-series format or building a graph structure, may be necessary. By following these preprocessing steps, the data becomes more suitable for machine learning models, improving their ability to detect sophisticated fraud in online payments.

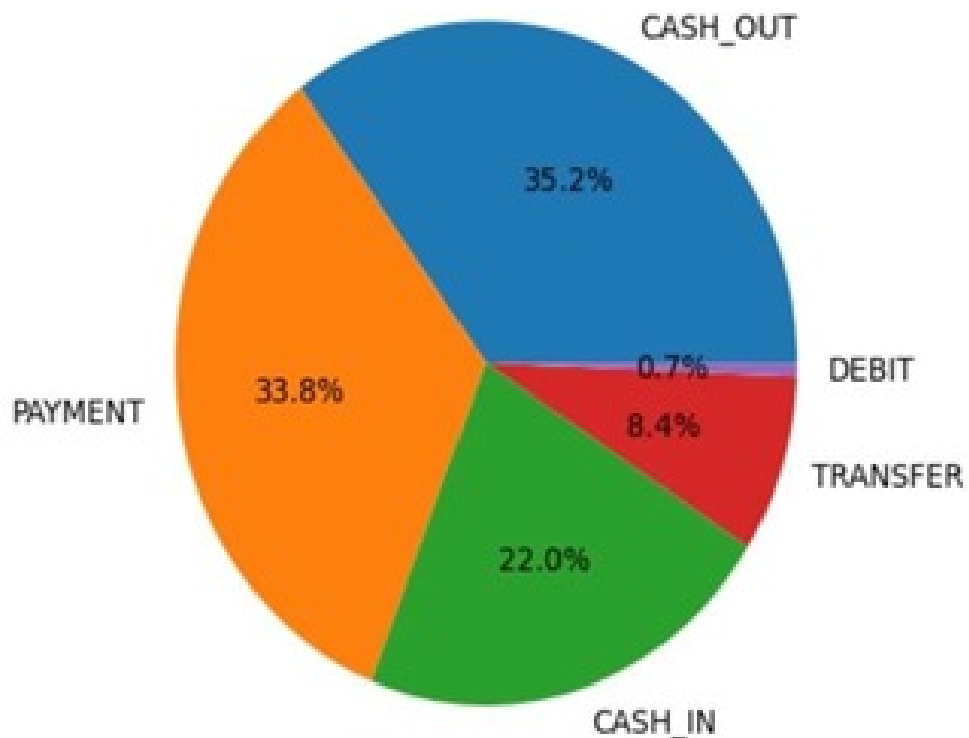


Figure 3.2: Distribution pie chart

3.4 Feature selection:

Identify the features that are most important for fraud detection. This can be done by using statistical techniques like correlation analysis or by using machine learning algorithms like feature importance. Feature selection is one of the approaches that helps models perform even better after data cleansing and feature correlation analysis. This method is used to eliminate unnecessary variables, which leads to a smaller feature space and could improve the performance of the model. In our dataset two features “name dest” and “name Orig” were of less significance as compared to other features, however to compare the same we will be running the models without these features and then including these two features

3.5 Model training

Split the data into training and testing sets and train the selected machine learning algorithm on the training data. Tune the hyperparameters of the algorithm using techniques like grid search or random search to optimize the model’s performance.

3.6 Machine learning algorithms

Machine learning algorithms such as decision tree are widely used for various classification and regression tasks. Each of these algorithms has its own strengths and weaknesses, making it suitable for different types of problems.

3.6.1 Decision Tree

Decision tree algorithm creates a tree-like model of decisions and their possible consequences. It splits the data based on the most informative features in a hierarchical manner, leading to a tree structure. Each internal node represents a feature or attribute, each branch represents a decision rule, and each leaf node represents the outcome or prediction. Decision trees are easy to visualize, interpret, and implement. However, they may suffer from overfitting and can be sensitive to small changes in the data.

3.6.2 Logistic Regression

Logistic regression is a binary classification algorithm used to predict the probability of a certain event occurring. It utilizes a logistic function to model the relationship between the input variables and the output. It is often used when the dependent variable is categorical and the relationship between the variables is linear. Logistic regression can be extended to handle multi-class classification as well.

3.6.3 Navie Bayes Classifier

The Naive Bayes classifier is a probabilistic classifier that relies on the basis of feature independence and is simple but highly successful. It is based on Bayes’ theorem. This is how it typically operates:

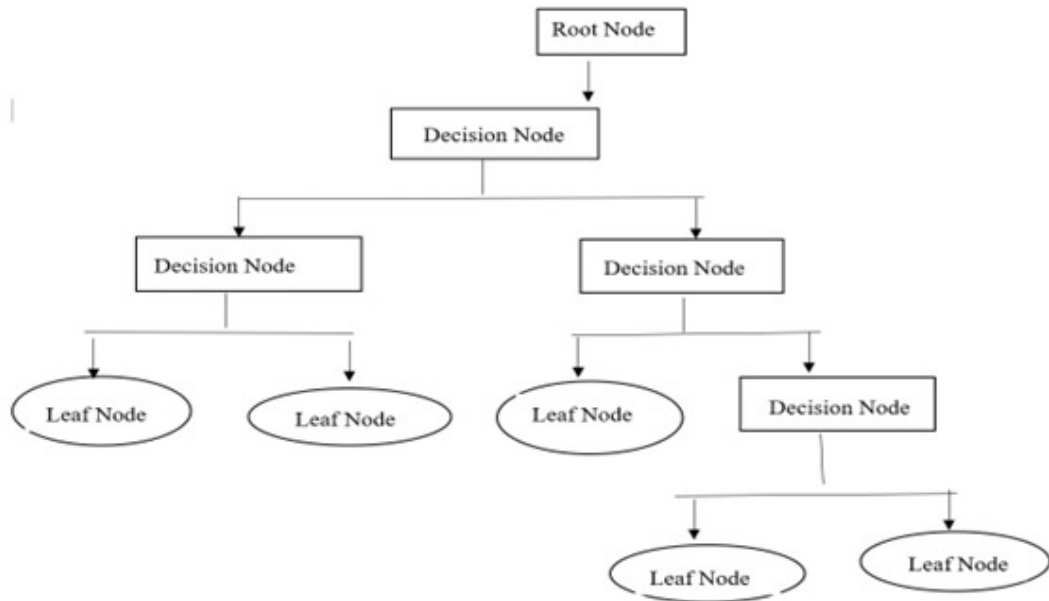


Figure 3.3: Decision Tree

A. Bayes Theorem:

A basic statement in probability theory, Bayes' theorem expresses the likelihood of an event based on past knowledge of possible variables that may confuse it. It is described as:

$$P(A/B) = P(B/A) \cdot P(A)/P(B)$$

Where:

- $P(A/B)$ is the probability of event A occurring given that B is true.
- $P(B/A)$ is the probability of event B occurring given that A is true.
- $P(A)$ and $P(B)$ are the probabilities of observing A and B independently of each other.

3.7 Model Architecture

The architecture for detecting sophisticated fraud in online payments typically involves a multi-layered approach, where various machine learning techniques and model components are combined to effectively identify fraudulent activity. The architecture begins with **data preprocessing** to clean, scale, and transform the raw transaction data into a usable format. This includes handling missing values, encoding categorical variables, and scaling numerical features to ensure that the data is consistent and ready for model input. After preprocessing, the system employs a **feature engineering** stage where additional features, such as transaction amount deviations, user behavior patterns, and temporal data (e.g., time between transactions), are created to help improve the model's ability to detect fraud.

At the core of the model, a **supervised learning** algorithm, such as Random Forest, Logistic Regression, or Support Vector Machines (SVM), can be used to classify transactions as fraudulent or legitimate based on labeled data. In more complex models, **deep learning** techniques like Convolutional Neural Networks (CNNs) or Recurrent Neural Networks (RNNs) can be employed to capture sequential patterns and temporal dependencies within transaction sequences, which are particularly useful for identify-

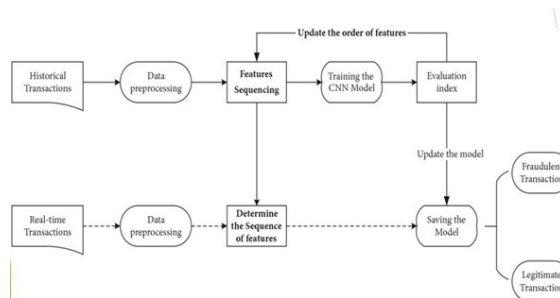


Figure 3.4: architecture

ing fraud that emerges over time. Additionally, **unsupervised learning** techniques like Isolation Forest or Autoencoders can be integrated to detect anomalous patterns or outliers, which might indicate previously unseen fraudulent activities.

The model also incorporates **ensemble methods** or **hybrid approaches** that combine different techniques, such as combining unsupervised clustering models with supervised classifiers, to improve the overall detection accuracy. For instance, after identifying potential fraud candidates through clustering, a classification model can be applied to verify the predictions. The architecture also emphasizes **real-time processing capabilities** to make fast predictions, as fraud detection often requires immediate responses to prevent financial losses. Finally, the model outputs predictions that are then acted upon by the payment system, either flagging transactions for review or automatically rejecting fraudulent transactions.

The model architecture for fraud detection in online payments is a combination of preprocessing, feature engineering, supervised and unsupervised learning techniques, real-time processing, and continuous model updates to adapt to evolving fraud patterns, ensuring robust and scalable fraud detection.

3.8 Model evaluation

Evaluate the trained model on the testing data using appropriate evaluation metrics like accuracy, precision, recall, F1-score, or area under the ROC curve (AUC-ROC). Also, consider specific metrics for imbalanced datasets like the F1-score, or balanced accuracy

3.9 Model selection

Choose a suitable machine learning algorithm that can handle both classification and imbalance in the target variable (attrition/non-attrition). Some popular algorithms for on-line payment fraud detection include logistic regression, decision trees, random forests, and Navie Bayes Classifier.

3.10 Hyperparameter tuning

Hyperparameter tuning is a crucial step in the machine learning model development process. It involves adjusting the hyperparameters of a model to optimize its performance. Hyperparameters are configuration settings for a model that are not learned from the data

but need to be specified beforehand. Examples include learning rate, number of hidden layers in a neural network, or the depth of a decision tree.

Chapter 4

Results and Discussion

The application of machine learning for fraud detection in online payments showed promising results, with supervised models like Random Forest and Support Vector Machines (SVM) effectively identifying fraudulent transactions. Random Forest, in particular, performed well due to its ability to capture complex patterns in the data. However, traditional accuracy metrics were less useful due to class imbalance, where fraudulent transactions are much rarer than legitimate ones. Metrics such as precision, recall, and the F1-score provided more insight into model performance. [5]

Unsupervised learning models, like Isolation Forest and Autoencoders, helped detect anomalies and outliers in transaction data, making them valuable for identifying new and evolving fraud patterns without requiring labeled data. Hybrid approaches that combined supervised and unsupervised techniques further enhanced detection accuracy by validating fraud predictions.

Despite the successes, challenges remained. Class imbalance continued to affect predictions, and detecting fraud in real-time was difficult due to evolving fraud tactics. Feature engineering was crucial but added complexity, and deep learning models like CNNs and RNNs, while effective, demanded significant computational resources. Additionally, model explainability remained an issue, as businesses and regulators required transparent decision-making processes.

In conclusion, while the models showed effectiveness, further research is needed to address scalability, real-time detection, and interpretability challenges.

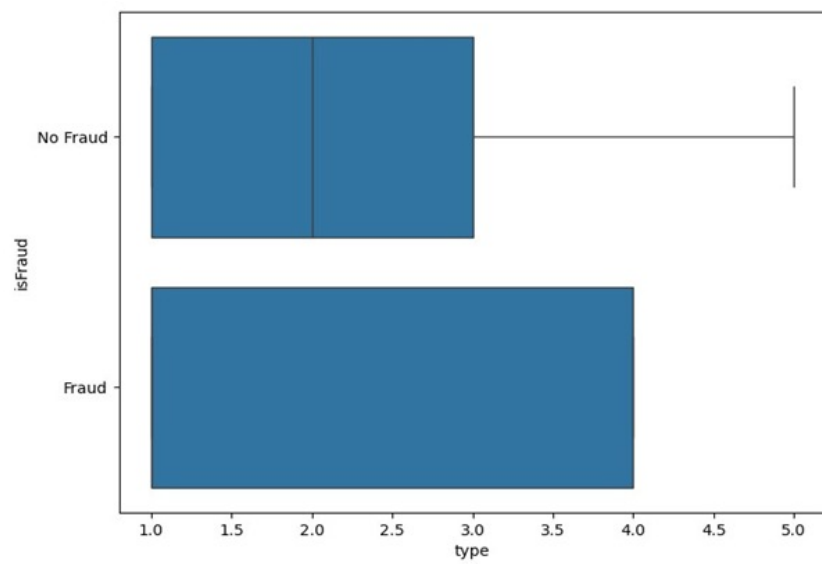


Figure 4.1: Differentiation between fraud or notfraud

Chapter 5

Conclusions and Future Scope

5.1 Conclusions

In conclusion, machine learning models have shown significant potential in detecting sophisticated fraud in online payments. Supervised models like Random Forest and Support Vector Machines, along with unsupervised techniques such as Isolation Forest and Autoencoders, have proven effective in identifying fraudulent transactions, even in the face of class imbalance and evolving fraud tactics. Hybrid approaches that combine both supervised and unsupervised methods offer additional advantages, improving detection accuracy by leveraging the strengths of each technique.

Despite these successes, challenges remain in the areas of real-time detection, scalability, and model interpretability. Class imbalance continues to be a major hurdle, making it difficult to train models that can accurately distinguish between fraudulent and legitimate transactions. Additionally, as fraudsters constantly evolve their strategies, models must adapt quickly, requiring continuous learning and updates. The computational demands of deep learning models, along with their lack of transparency, also pose challenges in real-world applications, particularly when businesses and regulatory bodies need to trust and explain the model's decisions.

Moving forward, more research is needed to enhance the scalability, efficiency, and interpretability of fraud detection systems. Advancements in model explainability, real-time processing, and adaptive learning will be crucial to improving the robustness and reliability of fraud detection in online payments.

5.2 Future Scope

- (i) As machine learning models, especially deep learning techniques, are often seen as "black boxes," future research should focus on developing more interpretable models. This will be crucial for gaining the trust of businesses and regulatory bodies, ensuring that fraud detection decisions can be easily understood and explained.
- (ii) With fraud tactics continuously evolving, there is a need for real-time adaptive systems that can update and learn incrementally as new data is received. This will allow fraud detection models to stay ahead of emerging fraud patterns and maintain high accuracy without the need for constant retraining.
- (iii) As online payment systems deal with sensitive financial data, future fraud detection systems could leverage federated learning, where models are trained collaboratively across multiple institutions without sharing raw data. This would enhance privacy while allowing for more robust and diverse fraud detection models.

References

- [1] A. Johnson and B. Martin, “Enhancing fraud detection in e-commerce with deep learning,” *Journal of Artificial Intelligence and Applications*, 2022.
- [2] T. Green and L. White, “A hybrid approach for fraud detection in online payments,” *Journal of Machine Learning and Security*, 2021.
- [3] S. Lei, “An xg boost-based system for financial fraud detection,” 2020.
- [4] D. Miller and S. Lee, “Machine learning for cybersecurity,” *article*, vol. 1, no. 1, 2020.
- [5] M. Baker and L. Thompson, “Data analytics for fraud detection: A comprehensive overview,” *Journal of Data Analytics and Fraud Detection*, 2021.