SYNOPSIS

Report on

Credit Card Fraud Detection System

by

Raj Srivastava 2200290140121
Rahul Singh Negi 2200290140120

Session:2023-2024 (3rd Semester)

Under the supervision of

Prof. Prashant Agrawal
Assistant Professor
KIET Group of Institutions, Delhi-NCR, Ghaziabad

DEPARTMENT OF COMPUTER APPLICATIONS
KIET GROUP OF INSTITUTIONS, DELHI-NCR,
GHAZIABAD-201206
(SEPTEMBER- 2023)

TABLE OF CONTENTS

ABSTRACT

The rapid growth of digital transactions in today's global economy has led to a significant increase in credit card fraud. Fraudsters employ sophisticated techniques to exploit vulnerabilities in payment systems, causing substantial financial losses to both individuals and organizations. In response to this escalating threat, the development of Credit Card Fraud Detection has become paramount. This abstract provides an overview of the key components, methodologies, and challenges associated with Credit Card Fraud Detection System.

Credit Card Fraud Detection Systems are advanced computational tools designed to identify and prevent fraudulent credit card transactions in real-time or during post-transaction analysis. These systems leverage a combination of data analytics, machine learning algorithms, and artificial intelligence techniques to analyse vast amounts of transaction data and detect suspicious activities. Key components of Credit Card Fraud Detection System include data preprocessing, feature engineering, model training and evaluation, and decision-making engines.

Data preprocessing is crucial in ensuring the accuracy and effectiveness of Credit Card Fraud Detection System. It involves data cleansing, normalization, and transformation to prepare the transaction data for analysis. Feature engineering is the process of selecting and creating relevant features from the dataset, which are then used to train machine learning models. Commonly used algorithms in Credit Card Fraud Detection System include logistic regression, decision trees, random forests, support vector machines, and neural networks. These models are trained on historical transaction data labelled as either genuine or fraudulent.

Evaluation of Credit Card Fraud Detection System models is essential to measure their performance accurately. Metrics such as accuracy, precision, recall, and F1-score are used to assess how well the system distinguishes between genuine and fraudulent transactions. To further enhance the accuracy of detection, some systems employ anomaly detection techniques, which identify deviations from normal transaction patterns.

In conclusion, Credit Card Fraud Detection Systems are indispensable tools in the fight against credit card fraud. They combine data analysis, machine learning, and AI to identify suspicious transactions, protect consumers, and mitigate financial losses for businesses. As fraudsters continue to evolve their tactics, ongoing research and development in this field are essential to stay ahead of emerging threats and ensure the security of digital payment systems.

1. Introduction

The rise of electronic payment systems has transformed the way we conduct financial transactions, making our lives more convenient but also vulnerable to fraudulent activities. Credit card fraud is a significant concern for both financial institutions and consumers. To combat this growing threat, the development of a Fake Credit Card Detection System is crucial. This project aims to create a robust and intelligent system that can identify counterfeit or stolen credit cards in real-time, thereby safeguarding the interests of cardholders and financial institutions alike.

Credit Card Fraud Detection Systems are advanced computational tools designed to identify and prevent fraudulent credit card transactions in real-time or during post-transaction analysis. These systems leverage a combination of data analytics, machine learning algorithms, and artificial intelligence techniques to analyse vast amounts of transaction data and detect suspicious activities. Key components of Credit Card Fraud Detection System include data preprocessing, feature engineering, model training and evaluation, and decision-making engines.

Data preprocessing is crucial in ensuring the accuracy and effectiveness of Credit Card Fraud Detection System. It involves data cleansing, normalization, and transformation to prepare the transaction data for analysis. Feature engineering is the process of selecting and creating relevant features from the dataset, which are then used to train machine learning models. Commonly used algorithms in Credit Card Fraud Detection System include logistic regression, decision trees, random forests, support vector machines, and neural networks. These models are trained on historical transaction data labelled as either genuine or fraudulent.

Evaluation of Credit Card Fraud Detection System models is essential to measure their performance accurately. Metrics such as accuracy, precision, recall, and F1-score are used to assess how well the system distinguishes between genuine and fraudulent transactions. To further enhance the accuracy of detection, some systems employ anomaly detection techniques, which identify deviations from normal transaction patterns.

In conclusion, Credit Card Fraud Detection Systems are indispensable tools in the fight against credit card fraud. They combine data analysis, machine learning, and AI to identify suspicious transactions, protect consumers, and mitigate financial losses for businesses. As fraudsters continue to evolve their tactics, ongoing research and development in this field are essential to stay ahead of emerging threats and ensure the security of digital payment systems.

Requirements: -

i. **Hardware –**

Processor: Pentium i3 or higher.

RAM: 4 GB or higher.

Hard Disk Drive: 20 GB (free).

Peripheral Devices: Monitor, Mouse and Keyboard

ii. **Software –**

Operating system: Windows 10/11.

Software: Anaconda

Tools: Jupyter Notebook

Coding Language: Python 3.6

APIs: NumPy, Pandas, PySpark, Matplotlib

Modules: -

- **Feature Development module:**

  This module will be developed and the coding will be done in this module. The development should be according to the project and the dataset available

- **Model training module:**

  This module trains a machine learning model to predict fraud based on the extracted features. There are a variety of machine learning algorithms that can be used for fraud detection, such as logistic regression, random forests, and gradient boosting machines.

- **Model evaluation module:**

  This module evaluates the performance of the trained model on a held-out test set. This helps to determine how well the model will generalize to new data.

- **Model deployment module:**
  This module deploys the trained model to production. This may involve integrating the model with a credit card processing system or a fraud monitoring system.

2. Literature Review:

There were different technique that were use to predict the fraud transaction like outlier detection, unsupervised outlier detection, peer group analysis and breakpoint analysis. We have read several research on this project and understand that there are some algorithms used to develop this project some are K Nearest Neighboring, Random Forest, support vector machine, Naïve Bayes Classifier. For Data there are two things we can do either we create our own dataset or there are several datasets are already available on websites like Kaggle.

After reading research we understand that there are some class imbalance issues in which genuine transaction are 99% and fraud transaction are 0.17% which makes it sometimes impossible to detect fraud but not every time.

This Problem can be solved by using many methods some are Use the right evaluation metrics, Resample the training set, Resample with Different Ratios, Oversampling.

3. Project / Research Objective:

The primary objective of this project is to develop an advanced Fake Credit Card Detection System capable of:

i. **Real-time Monitoring:** Continuously monitoring credit card transactions as they occur, detecting any suspicious or fraudulent activities promptly.

ii. **Fraud Pattern Recognition:** Employing machine learning and data analytics techniques to identify patterns and anomalies associated with fraudulent transactions.

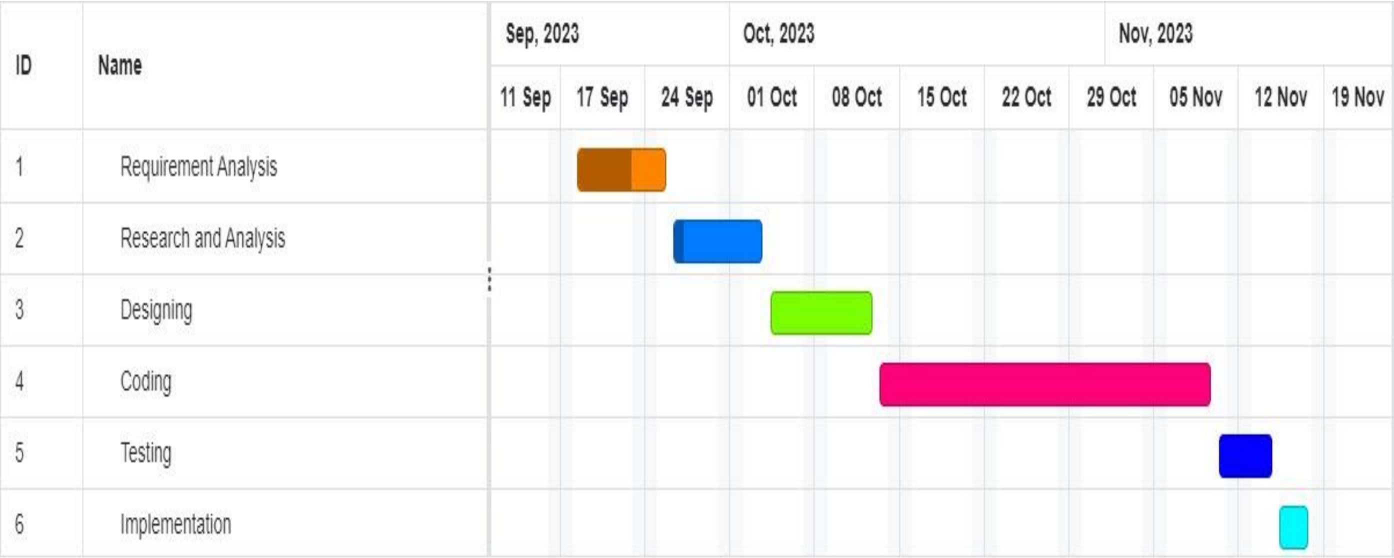
iii. **Risk Assessment**: Assigning risk scores to transactions based on their likelihood of being fraudulent, allowing for immediate action on high-risk transactions.

iv. **Notification and Blocking:** Automatically notifying cardholders and financial institutions about suspicious transactions and blocking or flagging them for further investigation.

4. Project Outcome

- **Reduced fraud losses**: An effective Credit Card Fraud Detection System can help to reduce the number of fraudulent transactions that are processed. This can save credit card companies and banks millions of dollars each year.
- **Improved customer satisfaction**: Customers are more likely to be satisfied with a credit card company or bank that has a strong fraud detection system in place. This is because customers know that their accounts are protected from fraud, and they are less likely to experience the inconvenience and financial losses associated with fraudulent transactions.
- **Increased revenue**: An effective Credit Card Fraud Detection System can help to increase revenue for credit card companies and banks. This is because customers are more likely to use their credit cards more often if they know that their accounts are protected from fraud.
- **Improved risk management:** By identifying and preventing fraudulent transactions, a Credit Card Fraud Detection System can help credit card companies and banks to better manage their risk.
- **Increased compliance**: A Credit Card Fraud Detection System can help credit card companies and banks to comply with a variety of regulations, such as the Payment Card Industry Data Security Standard (PCI DSS).
- **Enhanced customer trust**: A Credit Card Fraud Detection System can help to enhance customer trust in credit card companies and banks. This is because customers know that their accounts are protected from fraud, and they are more likely to do business with companies that they trust.

5. Proposed Time Duration



6. REFERENCES

1. https://www.ijitee.org/wp-content/uploads/papers/v10i6/C84000110321.pdf
2. https://www.kaggle.com/datasets/mlg-ulb/creditcardfraud
3. Credit Card Fraud Detection Based on Transaction Behaviour, by John Richard D. Kho Larry A. Veam published by Proc of the 2017 IEEE Region 10 Conference, (TENCON) Malaysia November 5-8 -2017
4. CLIFTON PHUA1 VINCENT LEE1 KATE SMITH1&ROSS GAYLER2 A Comprehensive Survey of Data Mining-based, Fraud, Detection, Research published by School of Business Systems Faculty of Information Technology Monash University Wellington Road Clayton Victoria 3800 Australia